Chambre des notaires du Québec

MÉMOIRE SUR L'AVANT-PROJET DE LOI, *LOI SUR LA NORMALISATION JURIDIQUE DES NOUVELLES TECHNOLOGIES DE L'INFORMATION*

PRÉSENTÉ

À LA COMMISSION DE L'ÉCONOMIE ET DU TRAVAIL

AOÛT 2000

Table des matières

SOMMAIRE DES RECOMMANDATIONS.....I

INTRODUCTION.....1

COMMENTAIRES GÉNÉRAUX.....4

ANALYSE INDIVIDUELLE DES ARTICLES.....5

LE TITRE DE LA LOI.....5
DISPOSITIONS GÉNÉRALES.....5

ARTICLE 1 par. 2º.....6

ARTICLE 2.....6
LA NOTION DE DOCUMENT.....7

ARTICLE 3.....7
LA FIABILITÉ DU DOCUMENT.....8

ARTICLE 5.....8
LA DÉTERMINATION DE LA VALEUR JURIDIQUE DU DOCUMENT.....10

ARTICLE 8.....10

ARTICLE 9.....13

ARTICLE 10.....13

ARTICLE 11.....14

ARTICLE 12.....16

ARTICLE 13.....17

ARTICLE 14.....19

ARTICLE 15.....19

ARTICLE 16.....20
LE MAINTIEN DE LA FIABILITÉ DU DOCUMENT.....20

EN COURS DE SON CYCLE DE VIE 20
ARTICLE 17 20
ARTICLE 18 22
ARTICLE 19 24
ARTICLE 25 25
ARTICLE 29 27
ARTICLE 35 28
ARTICLE 36 30
ARTICLE 37 31
ARTICLE 38 33
ARTICLES 39 ET 40 34
LES MOYENS DE RELIER UNE PERSONNE 35
ET UN DOCUMENT TECHNOLOGIQUE 35
ARTICLE 41 35
ARTICLE 44 35
L'IDENTIFICATION ET LE REPÉRAGE DES PERSONNES, DES DOCUMENTS ET DES AUTRES OBJETS SERVANT À LA COMMUNICATION 37
ARTICLE 45 37
ARTICLE 49 38
ARTICLE 50 40
ARTICLE 51 42
LA CERTIFICATION 45
ARTICLE 54 45
ARTICLE 55 46
ARTICLES 58 ET 59 47
ARTICLE 60 48

ARTICLE 61 49
ARTICLE 62 50
ARTICLE 63 51
ARTICLE 64 52
ARTICLE 65 53
ARTICLE 66 54
ARTICLE 67 54
ARTICLE 70 56
ARTICLE 71 57
ARTICLE 73 58
ARTICLE 74 58
ARTICLE 75 59
CONCLUSION 60
Annexe 1

AVANT PROJET DE LOI, *LOI SUR LA NORMALISATION JURIDIQUE DES NOUVELLES TECHNOLOGIES DE L'INFORMATION*

SOMMAIRE DES RECOMMANDATIONS

Dans le cadre de l'analyse de l'Avant-projet de loi*, Loi sur la normalisation juridique des nouvelles technologies de l'information*, la Chambre des notaires propose notamment les modifications suivantes :

- **QU**'une liste de définitions soit incluse dans l'avant-projet de loi, au moins pour les éléments techniques ou pour les nouvelles notions qui y sont introduites;

- **QU**'un préambule soit inclus dans l'avant-projet de loi aux termes duquel on retrouverait l'article 1, lequel devrait être complété par d'autres articles qui permettraient de dresser un portrait d'ensemble de tous les principes qui le gouvernent;

- **QUE** le titre de la loi soit amélioré, notamment en retirant le mot « nouvelles »;

- **QUE** l'article 2, qui contient une règle de droit et constitue un principe de base fondamental, demeure en tout temps au cœur de la loi, puisqu'il assure à l'ensemble des citoyens le droit de communiquer avec les instances gouvernementales selon le mode qui leur convient, que le projet de loi soit gouverné par ce principe et qu'il ne soit pas contrecarré par l'adoption de lois qui auraient pour effet d'obliger, en certaines occasions, les citoyens à avoir recours aux technologies de l'information;

- **QUE** les mots « fiabilité » et « intégrité » soient définis et que, dans l'appréciation de l'intégrité d'un document, plusieurs autres éléments et non pas seulement les mesures de sécurité soient utilisés (art. 5.);

- **QUE** la section portant sur la « Détermination de la valeur juridique du document » soit déplacée à la fin du Chapitre 1, puisque la valeur juridique d'un document s'évaluera également en fonction du maintien de sa fiabilité au cours de son cycle de vie.

- **QUE** dans la mesure où la condition de fiabilité est rencontrée, le document sous forme de son et d'image bénéficie du même traitement que les autres (art. 8);

- **QUE** les articles 8 et 9 soient modifiés afin d'éclaircir la notion de « valeur juridique » d'un document fiable;

- **QUE** l'article 11 soit retranché de l'avant-projet de loi, puisque les éléments qui y sont précisés se retrouvent dans les sections relatives au maintien de la fiabilité du document durant son cycle de vie;

- **QUE** l'article 12 soit modifié notamment afin de s'assurer que des dispositions d'autres lois requérant l'apposition d'un sceau ne puissent rendre inutilisables le médium informatique;

- **QUE** l'article 13 soit déplacé dans la section portant sur le transfert de l'information et qu'on lui accorde la présomption de fiabilité si elle rencontre les règles prévues relativement au transfert de l'information afin d'éviter de créer deux séries de règles distinctes pour des opérations similaires;
- **QUE** l'article 14 soit modifié afin d'y retrancher les méthodes à utiliser en ne stipulant que la méthode à utiliser pour certifier la conformité d'une copie doit être compatible avec le support du document certifié;

- **QUE** la notion ***« d'un transfert vers un support faisant appel à une technologie différent »*** soit retranchée et remplacée par celle du document de travail, soit « ...*pour qu'un document dont l'information a fait l'objet d'un transfert puisse être détruit et remplacé par un document intègre porteur de la même information* (art. 17) »;

- **QUE** les plus petites entreprises soient assimilées aux particuliers afin qu'elles soient libérées des obligations plus importantes de l'alinéa 1. Le nombre d'employés, le fait de percevoir les taxes, etc., pourraient fournir des exemples de critères de distinction à un tel allégement (art. 17);

- **QUE** soient exclues les petites entreprises relativement aux exigences posées par l'article 18;

- **QUE** l'article 19 soit retranché, puisque l'article 18 y pourvoirait en retirant les mots « sauf dans les cas prévus à l'article 19 »;

- **QUE** les mots « conservés par ce dernier » soient remplacés par le mot « remisé », comme dans le document de travail (art. 25);

- **QUE** tous les articles concernant la responsabilité des intermédiaires et des autres intervenants soient rassemblés en une seule section;

- **QUE** la responsabilité de l'expéditeur soit limitée à s'assurer que les copies sont identiques au moment de la transmission (art. 35);

- **QUE** le dernier alinéa de l'article 35 soit retranché;

- **QUE** le terme « personne physique », qui correspond à une notion existante au Code civil, soit utilisé partout dans l'avant-projet de loi à la place du mot « particulier » (art. 36);

- **QUE** la présomption de fiabilité bénéficie à toute personne et non pas seulement au particulier (art. 36);

- **QUE** le deuxième alinéa de l'article 37 soit retiré, les alinéas 1 et 3 étant suffisants à créer l'obligation de protéger les renseignements confidentiels;

- **QUE** l'article 38 soit revu et qu'on y apporte notamment des précisions quant à l'origine de l'erreur;

- **QUE** l'inopposabilité d'une transaction effectuée avec une biclé ne soit admise qu'au cas où la clé privée a été utilisée sans droit ou frauduleusement (art.44.);

- **QUE** l'on prévoit l'impossibilité d'exiger l'établissement de l'identité d'un individu au moyen *d'un procédé ou d'un dispositif qui porte atteinte à son intégrité physique* (art. 49);

- **QU**'il soit interdit qu'une loi puisse faire fi de cette règle générale en permettant expressément que l'identité d'une personne soit établie au moyen d'un dispositif portant atteinte à son intégrité physique, sauf dans des circonstances exceptionnelles permettant d'utiliser un tel procédé afin de localiser en tout temps un criminel;

- **QUE** la Commission d'accès à l'information puisse exercer à priori son pouvoir sur toute création d'une banque de caractéristiques ou de mesures biométriques et que la création d'une telle banque fasse l'objet d'une analyse approfondie sur son opportunité et de recommandations sur les conditions qui devraient encadrer sa constitution, son maintien et son opération (art. 50);

- **QUE** le pouvoir accordé à la Commission de rendre toute ordonnance soit obligatoire (art. 50);

- **QUE** cette banque soit gérée exclusivement par un organisme gouvernemental, redevable envers la population et seul à pouvoir s'assurer que les informations qui y seraient contenues fassent l'objet de toutes les mesures de protection possibles (art. 50);

- **QUE** des précisions soient apportées à l'article 51 notamment en ce qui concerne les notions de « espace nominatif local et espace nominatif universel »;

- **QUE** le deuxième alinéa de l'article 63 soit retiré;

- **QUE** l'article 64 soit retiré;

- **QU**'en l'absence de faute, le prestataire de services ne soit pas tenu de réparer ni en totalité ni en partie le préjudice (art. 65);

- **QUE** siègent sur le comité prévu à l'article 67, des représentants du milieu juridique, plus particulièrement des juristes versés en droit des nouvelles technologies de l'information;

- **QUE** le comité de concertation prévu au document de travail soit créé, puisqu'il permettrait à des intervenants de différents milieux de faire part de leurs préoccupations en la matière;

- **QUE** la notion de « dossier » soit précisée (art. 70);

- **QUE** l'alinéa 1 de l'article 70 soit modifié en remplaçant l'énumération prévue par une règle générale;

- **QUE** l'article 71 soit intégré à l'article 11.

PROJET DE LOI, *LOI SUR LA NORMALISATION JURIDIQUE DES NOUVELLES TECHNOLOGIES DE L'INFORMATION*

INTRODUCTION

À sa première lecture, l'Avant-projet de loi, *Loi sur la normalisation juridique des nouvelles technologies de l'information* nous inspire des satisfactions au nombre desquelles, nous comptons la recherche de l'incontournable neutralité technologique, sans laquelle cet exercice législatif pourrait devenir désuet quand la technologie actuelle sera dépassée, c'est-à-dire dans très peu de temps. Nous notons également le soucis de protéger les consommateurs et les individus moins familiers avec les nouvelles technologies de l'information contre leur implantation forcée, qui permettra à tous nos concitoyens de s'adapter à leur rythme aux nouvelles règles du jeu qui en découlent. Nous saluons aussi l'alignement vers certains principes internationaux en la matière, notamment ceux qui se retrouvent à la loi type de la Commission des Nations Unies pour le droit commercial international (CNUDCI) sur le commerce électronique[1], repris dans la *Loi uniforme sur le commerce électronique*[2] de la Conférence pour l'harmonisation des lois au Canada, ou encore à la *Loi uniforme sur la preuve électronique*[3] de cette même organisation.

Nous applaudissons à la détermination du gouvernement à doter le Québec d'un cadre juridique qui vise à encourager le virage technologique en sécurisant l'aspect juridique. L'Union Européenne, plusieurs pays, États américains et autres juridictions canadiennes l'ont déjà fait, ou sont en train de le faire. Les plus récents efforts en ce sens proviennent des gouvernements de la Colombie-Britannique[4] et, non le moindre,

[1] http ://www.uncitral.org/french/texts/electcom/ml-ec.htm#TOP.
[2] http ://www.law.ualberta.ca/alri/ulc/current/fueca99a.htm#3.
[3] http ://www.law.ualberta.ca/alri/ulc/current/feeact.htm.
[4] http ://www.legis.gov.bc.ca/2000/1st_read/gov32-1.htm.

des États-Unis[5]. Le Québec, qui rattache de plus en plus son développement économique à la locomotive de la nouvelle économie du savoir et de la nouvelle technologie, ne peut se passer d'une telle loi.

Mais, il nous faut mettre de côté pour quelques instants notre enthousiasme envers cette initiative et mettre notre sens critique au service de l'amélioration de cette loi majeure. Si notre satisfaction a été soulevée par l'intention de la loi, nos remarques découlent principalement de sa rédaction trop souvent tortueuse et hermétique. Il relève désormais du lieu commun de déclamer sur le caractère international du Web. Les transactions peuvent s'y produire à l'échelle planétaire, en quelques instants. Par des opérations simples, des biens sont vendus, des services sont rendus et des paiements sont effectués. Des sites marchands peuvent déménager d'un pays à un autre tout aussi facilement. Il est impératif dans un tel contexte que les lois des différents États, sans chercher à être identiques, puissent être compatibles et tout au moins, ne pas créer d'embûches indues par une trop grande complexité.

Le gouvernement cherche à entourer l'usage des nouvelles technologies d'une aura de confiance. Nous croyons que cette confiance doit reposer sur une compréhension de la loi et qu'une rédaction abordable est la meilleure façon d'y arriver. Nous sommes tout à fait conscients que le domaine des nouvelles technologies n'est pas le plus simple à décrire, surtout en respectant l'objectif nécessaire de neutralité recherché. Mais, nous sommes quand même persuadés qu'il est possible d'améliorer la rédaction de l'avant-projet de loi pour le rendre plus compréhensible. Nous notons en effet dans le texte déposé de fréquents manques de clarté et des répétitions inutiles. L'ordre de présentation des articles laisse aussi parfois à désirer, en disséminant des articles traitant du même sujet de base à plusieurs endroits du texte. Le résultat est malheureusement, dans de nombreux cas, un texte inutilement compliqué, qui sera inaccessible pour la plupart des citoyens et entraînera de nombreux recours judiciaires. La loi québécoise se doit d'être au moins aussi claire que celles des autres juridictions

[5] http ://thomas.loc.gov/cgi-bin/query/C ?c106 :./temp/~c106yPXY5a.

qui lui font concurrence dans la nouvelle économie. Nous espérons donc que nos observations permettront d'alléger et de clarifier cet avant-projet pour le bien-être de nos concitoyens.

Dans un autre ordre d'idées, nous relevons aussi l'excellente compréhension du gouvernement face à l'importance de la certification dans le cyberespace. Cette partie de la loi suscite le plus vif intérêt pour les notaires. L'implication traditionnelle du notariat dans la société québécoise et sa recherche constante de la plus grande sécurité pour les transactions qui l'animent, nous interpellent directement. Nous sommes convaincus de l'importance du rôle que la profession notariale peut jouer dans l'encadrement du commerce électronique et dans la stabilité des transactions virtuelles, notamment par le biais de la certification d'identité. Nous produisons d'ailleurs, en annexe, un texte vous présentant notre vision dans ce domaine.

De tous temps, le notariat d'ici a vécu au rythme de la société québécoise. De par son implication sociale et économique certes, mais également par la présence rassurante qu'il a su maintenir auprès de tous nos concitoyens, des plus fortunés aux plus modestes. Nous abordons maintenant une ère nouvelle, où nos habitudes seront bouleversées, nos certitudes ébranlées. Le notariat québécois souhaite continuer à y jouer son rôle et demeurer un facteur de stabilité et de sécurité sur lequel tous pourront se fier, tout particulièrement les parties les plus faibles aux transactions. Aussi, nous souhaitons manifester à l'égard de certaines dispositions, des objections, observations et conseils qui viseront à maintenir l'équilibre entre les différents intervenants.

Nous vous présenterons donc nos commentaires sur certains articles de « l'Avant-projet de loi, *Loi sur la normalisation juridique des nouvelles technologies de l'information ».* Nous souhaitons sincèrement que ces observations seront utiles à la préparation du projet de loi qui devrait suivre. De tels exercices étant par nature plutôt ingrats, nous tenons à répéter une dernière fois, avant de vous transmettre nos commentaires, notre

satisfaction de voir que le Québec confirmera son ouverture vers l'avenir en se dotant d'un texte maître dans ce domaine. Voici donc nos commentaires.

COMMENTAIRES GÉNÉRAUX

L'avant-projet de loi, de son propre aveu, recherche la neutralité technologique. Autrement dit, il évite sciemment de nommer directement des technologies existantes, afin d'éviter de les suivre dans la désuétude lorsqu'elles seront remplacées par d'autres. Nous approuvons ce choix. Cependant, cette quête de la neutralité entraîne l'obligation de décrire les buts recherchés par chaque technique ou, encore, les processus qu'elles impliquent et qui généralement leur survivront. Il faut donc accepter de voir s'alourdir le texte.

Dans ce contexte, tout en considérant les sujets très techniques abordés dans cet avant-projet de loi, nous croyons que malgré la tendance générale contraire, il serait très utile d'inclure une liste de définitions au document, au moins pour les éléments techniques (support, transfert, etc.) ou pour les nouvelles notions qui y sont introduites (fiabilité, intégrité, etc.). Il s'ensuivrait une moins grande incertitude quant à l'interprétation possible des dispositions et une simplification de plusieurs articles qui pourraient utiliser des termes déjà définis. Cela s'impose d'autant plus qu'un des objectifs du gouvernement est de « (…) facilite(r) l'accès aux règles de droit et permettre aux citoyens, aux entreprises et à l'État de se référer à un régime juridique intégré[6] ».

Les dispositions générales contiennent déjà, indirectement, certaines définitions. Nous croyons que plus de termes devraient être définis et que ces définitions devraient être regroupées.

[6] Ministère de la Justice, Document de travail accompagnant le projet de loi, *Loi sur la normalisation juridique de l'Inforoute* p. 9.

ANALYSE INDIVIDUELLE DES ARTICLES

LE TITRE DE LA LOI

Le titre choisi, soit *La Loi sur la normalisation juridique des nouvelles technologies de l'information,* nous semble constituer une amélioration par rapport à son prédécesseur, soit *Loi sur la normalisation juridique de l'inforoute*. En effet, cette loi couvre une réalité beaucoup plus large que l'inforoute puisqu'elle vise à réglementer l'usage des nouvelles technologies de l'information, que ce soit sur le Web ou non. Il pourrait cependant être amélioré, notamment en retirant le mot « nouvelles », qui sera rapidement désuet... Nous pourrions aussi penser à une « Loi sur le cadre juridique des technologies de l'information » ou encore, penser à utiliser dans le titre la notion « d'équivalences juridiques » qui est souvent entendu dans ce contexte. Mais le titre, tel qu'il est, pourrait aussi nous être acceptable.

DISPOSITIONS GÉNÉRALES

C'est avec une certaine surprise que nous avons pris connaissance du texte des dispositions générales. Nous avons constaté qu'elles reprennent en partie les énoncés du document explicatif joint au document de travail qui nous avait d'abord été transmis et qu'elles ne contiennent pas, sauf exception, des règles de droit, mais plutôt des principes généraux qui s'harmonisent avec difficulté au reste du projet. Nous sommes d'avis que l'article 1 ne devrait pas se trouver dans le corps de la loi, mais plutôt en préambule. Il nous apparaît, par ailleurs, indispensable qu'il soit complété par d'autres articles qui permettraient de dresser un portrait d'ensemble de tous les principes gouvernant ce projet. En somme, les principaux points traités dans le document explicatif devraient se retrouver dans ce préambule pour assurer aux lecteurs une meilleure compréhension de la loi qui nous semble être à toutes fins pratiques inaccessible pour la très grande majorité des citoyens.

ARTICLE 1 par. 2º

> **(…)**
>
> **2º la cohérence des règles de droit (…) qu'elles soient électronique, magnétique, optique, sans fil ou autres, ou qu'il s'agisse de microformes ou d'une combinaison de technologies.**

Nous nous interrogeons sur le sens qu'il faut donner au mot « microformes » dans cette disposition. Il serait utile d'en donner une définition pour fins de compréhension.

ARTICLE 2

> **2. À moins que la loi n'exige l'emploi exclusif d'un support particulier, un document peut être sur tout support. Ainsi, l'exigence d'un écrit n'emporte pas l'obligation d'utiliser un support particulier.**
>
> **Chacun peut utiliser les supports et les technologies de son choix, dans la mesure où ce choix respecte la règle de droit.**

L'article 2 du projet de loi contient une règle de droit et constitue un principe de base fondamental qui doit demeurer en tout temps au cœur de la loi, puisqu'il assure à l'ensemble des citoyens le droit de communiquer avec les instances gouvernementales selon le mode qui leur convient. Il nous apparaît essentiel que le projet de loi soit gouverné par ce principe et qu'il ne soit pas contrecarré par l'adoption de lois qui auraient pour effet d'obliger, en certaines occasions, les citoyens à avoir recours aux technologies de l'information, (voir, par exemple les articles 31 et 34).

Il serait contraire aux principes moraux édictés aux Chartes des droits et libertés que par l'effet d'une loi particulière, des citoyens, à qui pour différentes raisons, les technologies de l'information sont inaccessibles, se voient refuser quelque demande que ce soit et n'aient tout simplement pas accès à un service en raison de leur

incapacité à satisfaire les exigences de la loi. De plus, il ne faudrait pas que ce principe contenu à l'article 2 du projet de loi soit abrogé avant plusieurs années, assurant ainsi à tous les citoyens de tous âges la possibilité d'avoir recours, à quelque étape de leur vie, à d'autres supports que les seules technologies de l'information.

LA NOTION DE DOCUMENT

ARTICLE 3

> **3. Constitue un document toute information délimitée et structurée de façon tangible ou logique, selon le support qui la porte, et qui est intelligible sous forme d'écrit, d'image ou de son. Il peut être rédigé au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles.**
>
> **Est assimilée au document toute banque de données dont les éléments structurants permettent la délimitation et la structuration de l'information qui y est inscrite.**

L'ensemble de cette disposition est rédigé de manière quelque peu hermétique, obligeant les lecteurs à une laborieuse relecture. Les concepts qui y sont énoncés sont abstraits, les termes utilisés, tels que « délimités », « structurés », « tangible », « logique », juxtaposés les uns aux autres, sans définitions, nous laissent incertains sur le sens général et spécifique qu'il faut leur donner. Nous comprenons que le législateur a eu le souci d'englober le plus grand nombre de possibilités afin d'éviter que l'avancement des technologies ne rende sa loi désuète. Nous croyons qu'à défaut d'une liste de définitions nous permettant de mieux comprendre le sens des mots utilisés, le législateur aurait avantage à rédiger l'ensemble du premier alinéa de façon plus simple afin de clarifier les exigences qui y sont contenues.

Quant au deuxième alinéa, en plus des commentaires que nous avons formulés relativement au premier alinéa, nous nous interrogeons sur le sens de l'expression « banque de données » et sur le fait qu'une banque de données soit assimilée à un document. Nous croyons que l'introduction de cette notion peut créer une certaine confusion. Pour notre part, il nous semble que la banque de données ne devrait pas être assimilable à un document puisqu'elle ne constitue en fait que le cadre ou le moyen qui permet d'emmagasiner des informations. Cela reviendrait à affirmer, si on voulait faire une comparaison imagée, que le classeur contenant des dossiers serait un document alors qu'il n'est qu'un meuble nous permettant de rassembler au même endroit des dossiers touchant un grand nombre de sujets.

La banque de données en soi ne peut, à notre sens, constituer un document, puisque par définition, elle est sans cesse modifiée par les éléments que nous y ajoutons ou retirons. Ne serait-ce pas plutôt les éléments que nous en extrayons pour certaines fins qui pourraient constituer un document ? Est-ce l'effet visé par le législateur ? Le résultat d'une recherche effectuée à partir d'une banque de données, à condition que la technologie employée permette qu'il soit sauvegardé et conservé, devrait-il constituer lui aussi un document ? Et les éléments relatifs à un même objet consignés à la banque ? Est-il nécessaire, ou souhaitable, d'assimiler la totalité de la banque à un document ? La banque de données n'a d'utilité que pour fins de recherche par l'utilisateur et c'est le résultat de cette recherche qui devrait se qualifier de document. Nous sommes donc d'avis que cette disposition mérite d'être modifiée afin de retrancher cette expression ou, encore, afin de lui apporter des éclaircissements.

LA FIABILITÉ DU DOCUMENT

ARTICLE 5

> **5. Est fiable, le document dont les composantes sont délimitées et structurées de manière à permettre d'en assurer l'intégrité durant tout son cycle de vie lequel va de sa création à sa**

> **conservation, y compris son archivage ou sa destruction, et comprend son transfert, sa consultation et sa transmission.**
>
> **L'intégrité d'un document est assurée lorsque, d'une part, il est possible de vérifier que l'information n'est pas altérée et qu'elle est maintenue dans son intégralité et, d'autre part, lorsque le support qui porte l'information lui procure la stabilité et la pérennité voulue.**
>
> **Dans l'appréciation de l'intégrité, il est tenu compte des mesures de sécurité prises pour protéger le document au cours de son cycle de vie.**

Tout au long de l'avant-projet de loi, nous avons constaté que le législateur utilise deux concepts qui peuvent paraître interchangeables, bien que nous soyons parfaitement conscients que l'on ait voulu leur attribuer un sens différent. Pour notre part, s'il y a deux mots que nous souhaitons voir définis, ce sont bien les mots « fiabilité » et « intégrité ». À plusieurs reprises dans ce document, et nous vous le signalerons chaque fois, nous avons été confrontés à tenter de faire la différence entre ces deux concepts qui se recoupent et qui nous semblent destinés à exprimer la même chose bien qu'ils soient fréquemment utilisés dans des sens différents et qu'ils ne soient définis qu'en les mettant en opposition.

Deuxièmement, l'usage du critère « lui procure (...) la pérennité voulue » apparaît à première vue un peu flou. Il y aurait lieu de préciser ce concept, puisqu'il constitue l'un des critères définissant l'intégrité, notion fondamentale dans l'avant-projet de loi.

Finalement, nous remarquons que cet article, dans l'appréciation de l'intégrité, semble ne vouloir tenir compte que des mesures de sécurité prises pour protéger le document pendant son cycle de vie. Nous croyons que plusieurs éléments seraient utiles pour apprécier l'intégrité d'un document donné. Le terme « sécurité » pourrait en englober certains et en exclure d'autres, selon la définition que l'on peut donner à ce terme. Ainsi, l'article ne vise-t-il que les conditions de conservation de l'ordinateur ou du disque où le

document est logé, que ce soit au niveau des conditions de son entreposage ou des mesures prises pour en interdire l'accès (sécurité logique), ou vise-t-il aussi les mesures logicielles prises pour son entreposage (failles ou « bogues » informatiques, protection anti-virus, etc.) ? Il y aurait lieu de préciser.

LA DÉTERMINATION DE LA VALEUR JURIDIQUE DU DOCUMENT

Après avoir effectué une analyse approfondie de l'avant-projet de loi, nous en arrivons à la conclusion que cette section devrait se retrouver à la fin du Chapitre 1, puisque manifestement la valeur juridique d'un document s'évaluera également en fonction du maintien de sa fiabilité au cours de son cycle de vie. Ainsi, la qualité du transfert de l'information, la conservation et la transmission du document ne sont pas étrangères à la valeur juridique qui lui sera accordée. Aussi, nous recommandons, afin d'améliorer la cohérence de la loi et une meilleure compréhension des lecteurs, de déplacer cette section à la fin du même chapitre.

De plus, nous vous suggérons également que l'article 15 de l'avant-projet de loi soit le premier article de cette section, puisqu'il établit la présomption de fiabilité. Suivraient alors les dispositions suivantes dans le même ordre qu'elles sont présentées.

ARTICLE 8

> **8. Un document fiable, quel qu'en soit le support, a pleine valeur juridique.**
>
> **Il peut constituer un moyen de preuve et être admis à titre de preuve écrite ou, s'agissant d'un document intelligible sous forme de son ou d'image, à titre d'élément matériel de preuve.**
>
> **Le document dont la fiabilité ne peut être affirmée ni déniée peut, selon les circonstances, être admis à titre de témoignage ou d'élément matériel de preuve et servir de commencement de preuve.**

A- Nous avons du mal à saisir pourquoi le document sous forme de son ou d'image n'aurait pas le même traitement que les autres documents en ne permettant pas qu'il bénéficie du même régime de preuve, particulièrement dans le cadre d'une loi ayant le but ultime de créer une notion de « document » qui ne soit pas dépendante du support choisi.

D'une part, à l'article 3, il est édicté que « Constitue un document toute information (…) et qui est intelligible sous forme d'écrit, d'image ou de son. » et, d'autre part, à l'alinéa de l'article 8, il est prévu que le document fiable, quel qu'en soit le support, a pleine valeur juridique. N'est-il pas quelque peu illogique de considérer qu'un document sous forme de son ou d'image, par ailleurs fiable, n'ait pas plus de valeur qu'un document sur un autre support et qui ne serait pas fiable ? Et comment concilier cette situation avec le fait que le document, s'il est fiable, est censé avoir pleine valeur juridique ?

Il ressort clairement de l'avant-projet de loi que le législateur ne souhaite pas établir d'hiérarchie entre les différents supports. Or, sur le plan de la preuve, un document sous forme de son ou d'image perd une partie de sa valeur en voyant sa capacité de constituer une preuve écrite grandement diminuée.

Imaginons le cas suivant : un créancier hypothécaire donne quittance totale et finale de toutes sommes dues en vertu de tel acte de prêt garanti par hypothèque, par le moyen d'une bande vidéo sur laquelle il serait filmé. En principe, ce document pourrait être qualifié de fiable et ainsi se voir reconnaître la pleine valeur juridique. Or nonobstant ce fait, en cas de litige, ce vidéo ne pourrait servir qu'à titre d'élément matériel de preuve. Si le document est fiable, mais que par ailleurs il ne bénéficie d'aucune plus-value sur le plan de la preuve, sa valeur comme document diminue et, du coup, en raison de ce traitement discriminatoire, son utilisation comme support sera forcément moins attrayante.

Nous sommes d'avis que dans la mesure où la condition de fiabilité est rencontrée, le document sous forme de son et d'image devrait bénéficier du même traitement que les autres.

B- Deuxièmement, l'usage à l'alinéa 2 de la locution « ***ne peut être affirmée ni déniée*** », nous apparaît hasardeuse. Nous avons en effet peine à imaginer les circonstances où un tel document pourrait exister en présence de la présomption découlant de l'article 15. Ce dernier stipule qu'il n'y a pas lieu de faire la preuve de la fiabilité d'un document, à moins que la partie adverse ne fasse la preuve d'une atteinte à son intégrité. Comment alors imaginer un document dont la fiabilité ne peut être affirmée ni déniée, alors que sa fiabilité n'a pas à être démontrée à moins qu'elle ait été effectivement déniée ? Ne devrait-on pas remplacer les mots « ne peut être affirmé ni dénié » par « a été dénié » ?

C- L'ordre de présentation des articles de cette section est aussi, selon nous, à revoir et cela toujours à des fins de clarté. Nous croyons que l'article 8 devrait se limiter à son premier alinéa. Les alinéas 2 et 3 de l'article 8 devraient devenir les alinéas 2 et 3 de l'article 15. Finalement, cet article 15 amélioré devrait suivre immédiatement l'article 8. Il s'ensuivrait la présentation suivante de ces dispositions :

> ***8. Un document fiable, quel qu'en soit le support, a pleine valeur juridique.***
>
> ***9. (ancien 15) Il n'y a pas lieu de faire la preuve de la fiabilité d'un document, à moins que celui qui la conteste n'établisse, par prépondérance de preuve, qu'il y a eu atteinte à l'intégrité du document.***

(Un document fiable) peut constituer un moyen de preuve et être admis à titre de preuve écrite ou, s'agissant d'un document intelligible sous forme de son ou d'image, à titre d'élément matériel de preuve.

Le document dont la fiabilité ne peut être affirmée ni déniée peut, selon les circonstances, être admis à titre de témoignage ou d'élément matériel de preuve et servir de commencement de preuve.

ARTICLE 9

9. Des documents sur des supports différents peuvent avoir la même valeur juridique si chacun d'eux est fiable et porte la même information. L'un peut remplacer l'autre et ils peuvent être utilisés simultanément ou en alternance. De plus, ces documents peuvent être utilisés aux mêmes fins, notamment à titre d'original ou de copie qui en tient lieu.

En cas de perte, un document peut servir à reconstituer l'autre.

Nous nous interrogeons sur la nuance qui est ici apportée à la valeur juridique d'un document fiable. En effet, l'article 8 édicte qu'un document fiable a pleine valeur juridique, alors que l'article 9 prévoit que des documents **peuvent** avoir cette valeur juridique s'ils sont fiables. Ces deux dispositions nous semblent inconciliables. S'ils sont fiables, ils ONT la même valeur juridique et ne se contenteront pas de POUVOIR l'avoir. La condition préalable est la fiabilité. Ainsi, cette condition remplie, il ne devrait plus y avoir aucun obstacle à leur accorder la pleine valeur juridique.

ARTICLE 10

10. En cas de divergence entre l'information d'un document ayant fait l'objet d'un transfert du support papier vers un autre

> **support et de celle du document qui en résulte, le document sur support papier prévaut.**
>
> **En cas de divergence entre l'information de deux documents qui sont sur des supports différents ou faisant appel à des technologies différentes et qui sont censés porter la même information, le document qui prévaut est celui dont il est possible de vérifier que l'information n'a pas été altérée et qu'elle a été maintenue dans son intégralité.**
>
> **Si ces règles ne permettent pas de déterminer quel document prévaut et, en l'absence de convention ou d'entente, le document qui dans les circonstances paraît le plus fiable prévaut.**

L'alinéa 1 de cet article accorde une primauté au support papier en raison de motifs qui demeurent, quant à nous, inconnus. Nous émettons l'hypothèse que le législateur présume du fait que l'altération qui pourrait être faite à un document serait forcément sur un autre support que le papier. Pourquoi ? Cette altération peut aussi facilement être apportée au support papier qu'à n'importe quel autre.

Par ailleurs, cette règle nous semble contradictoire avec l'ensemble du projet qui suggère clairement que tous les supports ont la même valeur à la condition d'être fiables. Nous recommandons, en conséquence, de supprimer le premier alinéa de cet article. Le deuxième alinéa stipule la seule solution acceptable : le document qui prévaudra est celui dont il est possible de vérifier que l'information n'a pas été altérée et qu'elle a été maintenue dans son intégralité qu'il s'agisse d'un document électronique ou papier.

ARTICLE 11

> **11. Lorsque doit être produit un document technologique qui doit avoir valeur d'original pour affirmer, soit que ce document constitue la source première d'une reproduction, soit le caractère**

unique du document, soit qu'il s'agit de la forme première d'un document associé à une personne, cette exigence est satisfaite lorsque l'intégrité du document est assurée, et

1* dans le premier cas, lorsque les composantes du document technologique source ont été identifiées lors de la reproduction et ont été conservées intactes;

2* dans le deuxième cas, lorsque les composantes du document ou son support sont structurés au moyen d'un procédé de traitement qui permet d'affirmer le caractère unique du document, notamment par l'inclusion d'une composante exclusive ou distinctive ou par l'exclusion de toute forme de reproduction du document;

3* dans le troisième cas, lorsque les composantes du document ou son support sont structurés au moyen d'un procédé de traitement qui permet à la fois d'affirmer le caractère unique du document, d'identifier la personne auquel le document est associé et de maintenir cette association au cours de tout le cycle de vie du document.

Les procédés visés aux paragraphes 2º et 3º du premier alinéa doivent être reconnus par un organisme de normalisation national ou international visé à l'article 69.

Nous sommes d'avis que cette disposition devrait être retranchée de l'avant-projet de loi, les éléments y étant précisés se retrouvant dans les sections relatives au maintien de la fiabilité du document durant son cycle de vie. Pourquoi, dans la section concernant la détermination de la valeur juridique du document, devrait-on intégrer des règles aussi précises qui auraient pour effet de figer dans le temps une situation qui risque d'évoluer ? Ne serait-il pas préférable d'édicter, dans cette section, des règles générales et de nous rapporter, en matière de preuve, aux règles établies dans les sections pertinentes ? En outre, il nous apparaît que les conditions exigées afin qu'un

document technologique ait valeur d'original – et nous nous interrogeons sur l'apparition soudaine de ce concept et de sa corrélation avec la fiabilité – sont d'une telle lourdeur qu'il sera à toutes fins pratiques quasi impossible de les rencontrer. Pour ces raisons, nous recommandons que cette disposition soit retranchée de l'avant-projet de loi.

ARTICLE 12

> **12. Lorsqu'un document doit être scellé au moyen d'un sceau, d'un cachet, d'un tampon, d'un timbre ou d'un autre instrument pour manifester la valeur d'original du document, cette exigence peut être satisfaite à l'égard d'un document technologique, au moyen d'un procédé qui permet d'assurer l'intégrité du document.**
>
> **Cependant, lorsqu'il s'agit de manifester la valeur d'original d'un document, il faut, sur le plan de la forme, faire appel aux caractéristiques propres au support qui porte l'information, telles l'emploi d'un papier d'un grain spécial ou l'apposition d'une marque ou d'une mention distinctive ou d'un procédé qui permet cette apposition.**

Nous retrouvons encore ici la notion de « valeur d'original » rencontrée dans l'article précédent. Nous vous avouons qu'il s'agit là d'un « concept » que nous comprenons mal, surtout lorsque nous le juxtaposons avec ceux de « fiabilité » et d' « intégrité ». Cette notion, comme celle de « copie », « duplicata », etc., nous apparaît d'ailleurs plutôt désuète dans le contexte des technologies de l'information. Plus précisément, nous ne sommes pas d'avis que le sceau, ou tout autre instrument du même type, permette en toutes circonstances de manifester la valeur d'original d'un document et en quoi cette exigence, si rencontrée, pourrait en assurer l'intégrité. Cette réalité propre aux méthodes traditionnelles ne devrait pas, selon nous, être transposée aux nouvelles technologies de l'information, surtout pour lui conférer des vertus qu'elle ne possédait pas de toutes façons.

Comme commentaire général, soulignons que cet article, à l'instar de certains autres, pêche un peu par excès de zèle. En effet, et c'est le principe des équivalences, le but de la loi ne devrait qu'être de fournir des équivalences légales à la transposition de notions du monde dit « réel » au monde technologique ou informatique. La préoccupation de l'avant-projet en matière d'apposition de sceaux devrait se limiter à s'assurer que des dispositions d'autres lois requérant l'apposition d'un sceau, ne puissent rendre inutilisable le médium informatique. Il suffirait donc de stipuler que l'utilisation d'une technique compatible au médium sur lequel le document est conservé suffit à remplir les exigences d'apposition de sceau sur un médium papier. Nous craignons donc que le 2e alinéa de l'article ait pour effet d'apporter des limites inutiles et contraignantes. Nous suggérons que cet article soit en conséquence modifié pour se lire comme suit :

> ***12. Lorsqu'un document doit être scellé au moyen d'un sceau, d'un cachet, d'un tampon, d'un timbre ou d'un autre instrument pour manifester la valeur d'original du document, cette exigence peut être satisfaite à l'égard d'un document technologique, au moyen d'un procédé faisant appel aux caractéristiques propres au support qui porte l'information.***

ARTICLE 13

> **13. Lorsque la production d'une copie d'un document technologique est permise, le procédé employé pour l'effectuer doit présenter des garanties suffisamment sérieuses pour assurer l'intégrité de la copie et le fait qu'elle comporte la même information que le document source.**
>
> **Il est tenu compte dans l'appréciation de l'intégrité de la copie des circonstances dans lesquelles elle a été faite ainsi que du fait qu'elle a été effectuée de façon systématique et sans lacunes ou conformément à un procédé qui s'appuie sur des normes ou**

standards techniques reconnus par un organisme de normalisation national ou international visé à l'article 69.

Cependant, au plan de la forme, la copie doit présenter les caractéristiques qui permettent de reconnaître qu'il s'agit d'une copie, soit par l'indication du lieu et de la date où elle a été effectuée ou du fait qu'il s'agit d'une copie, soit par tout autre moyen.

La copie bénéficie d'une présomption de fiabilité en faveur des tiers du seul fait qu'elle a été effectuée par une entreprise au sens du Code civil ou par l'État.

Ici encore, nous sommes d'avis que cette disposition devrait se retrouver dans la section portant sur le transfert de l'information. Pourquoi, en effet, créer un régime spécial pour la copie, alors qu'il ne s'agit en fait que d'un transfert d'information dont les règles sont déjà établies ailleurs dans l'avant-projet de loi. Il nous semble plus logique de lui accorder la présomption de fiabilité si elle rencontre les règles prévues relativement au transfert de l'information et d'éviter de créer deux séries de règles distinctes pour des opérations similaires.

L'article pourrait se retrouver à la section relative au transfert d'information et se lire simplement comme suit :

Lorsque la production d'une copie d'un document technologique est permise, cette copie doit se faire selon les dispositions de la présente sous-section.

De plus, nous nous questionnons sur l'opportunité de n'accorder la présomption de fiabilité qu'aux copies réalisées par des entreprises ou par l'État si les mêmes conditions sont rencontrées.

ARTICLE 14

> **14. Lorsque la copie d'un document doit être certifiée ou vidimée, cette exigence peut être satisfaite à l'égard d'un document technologique, non seulement par collationnement visuel ou manuel, mais au moyen d'un procédé de comparaison permettant de reconnaître que l'information de la copie est identique à celle du document source ou que leurs empreintes respectives sont identiques.**

Ici aussi, les notions « d'original », de « copie » et la pertinence de les utiliser dans le contexte des technologies de l'information doit se poser. Cet article nous semble un peu trop précis. L'élaboration de règles entourant la production de copies certifiées relève selon nous de lois particulières visant des domaines particuliers (la *Loi sur le notariat* et ses règlements par exemple). La règle sur la production de copies et le transfert d'information sont déjà établies. La règle établissant que la copie doit comporter la même information que « l'original » se retrouve à l'article 13. La seule différence ici est qu'une personne doit se prononcer, au moment de la production de la copie pour certifier que cette exigence a été remplie. Le moyen qu'il utilisera pour vérifier la conformité de la copie relève selon nous de son choix, puisqu'il en portera la responsabilité. Il est donc superflu de stipuler les méthodes à utiliser. Il suffirait de stipuler que la méthode utilisée pour certifier la conformité d'une copie doit être compatible avec le support du document certifié.

ARTICLE 15

> **15. Il n'y a pas lieu de faire la preuve de la fiabilité d'un document, à moins que celui qui la conteste n'établisse, par prépondérance de preuve, qu'il y a eu atteinte à l'intégrité du document.**

Le retour de la notion d'intégrité dans cet article vient selon nous limiter la portée de possibles contestations à la fiabilité d'un document. Une référence aux conditions

établies aux articles 5 et suivants quant à la fiabilité engloberait mieux le concept. Ainsi, il y aurait présomption de fiabilité à moins que la partie adverse ne puisse établir que le document n'est pas fiable au sens des articles 5 à 7.

Nous vous référons aussi à nos commentaires ci-dessus relativement à l'article 8.

ARTICLE 16

> **16. Les procédés, systèmes ou technologies utilisés pour communiquer au moyen d'un document technologique n'ont pas à être prouvés, même en cas de contestation de la fiabilité du document, lorsqu'ils sont indiqués dans un décret du gouvernement, pris après consultation du comité visé à l'article 67, en y précisant leur application, la durée de leur utilisation ainsi que la norme ou le standard choisi.**
>
> **Toutefois, cette dispense n'empêche pas celui qui conteste la fiabilité d'un document, d'établir, par prépondérance de preuve, une erreur dans l'utilisation ou un dysfonctionnement dans l'application de ces procédés, systèmes ou technologies.**

Nous notons l'amélioration sensible de cet article par rapport à son prédécesseur (17) du document de travail. L'expression «...*communiquer au moyen d'un document technologique* » semble cependant un peu nébuleuse et mériterait d'être précisée.

LE MAINTIEN DE LA FIABILITÉ DU DOCUMENT EN COURS DE SON CYCLE DE VIE

ARTICLE 17

> **17. Sauf dans le cas prévu à l'article 19, pour qu'un document, original ou copie, dont l'information a fait l'objet d'un transfert vers un support faisant appel à une technologie différente puisse être détruit et remplacé par le document qui résulte du transfert et qui porte la même information, le transfert doit :**

> **1° dans le cas d'une personne morale, d'une société, d'une association ou de l'État, être préalablement autorisé par une personne qui y est en autorité ou qui est responsable de la conservation du document et être appuyé par de la documentation laquelle doit être disponible pour production en preuve;**
>
> **2° dans le cas d'un particulier, être précédé d'une vérification du fait que le support et la technologie dont il dispose pour effectuer le transfert sont assortis de garanties quant à la préservation de la même information que celle du document devant être transféré et quant à la préservation de l'intégrité, tant du document devant être transféré, s'il n'est pas détruit, que du document résultant du transfert il ne peut être requis, sous réserve d'un règlement pris en vertu de l'article 20, de fournir en preuve d'autre documentation relative au support ou aux technologies dont il dispose que celle rendue disponible par les fournisseurs.**

A- L'introduction de la notion ***« d'un transfert vers un support faisant appel à une technologie différente »*** nous paraît malheureuse. Elle vient limiter la portée de l'article par rapport à son prédécesseur au document de travail (22), qui stipulait quant à lui « ...*pour qu'un document dont l'information a fait l'objet d'un transfert puisse être détruit et remplacé par un document intègre porteur de la même information*. »

Le terme « technologie » est beaucoup trop vague et laisse trop place à interprétation. Ainsi, si un individu procède par exemple à un transfert d'information d'un document sous format Word vers un autre document de format Word, fait-il appel à une technologie différente ? Qu'en sera-il du transfert d'un format de traitement de texte vers un format de chiffrier ou de banque de données ? Il pourra s'agir en tous les cas de technologie informatique, bien que les logiciels particuliers utilisés peuvent être tout à fait incompatibles. Pourra-t-il détruire le fichier source ? L'usage de l'expression « technologie différente » serait à repenser, pour se rapprocher plus de celle contenue au document de travail.

B- Deuxièmement, le remplacement du terme « entreprise » par « personne morale » est bénéfique, le terme étant beaucoup plus précis. Nous nous demandons cependant s'il n'y aurait pas lieu d'assimiler les plus petites entreprises aux particuliers, et de les libérer des obligations plus importantes de l'alinéa 1. Le nombre d'employés, le fait de percevoir les taxes, etc., pourraient fournir des exemples de critères de distinction à un tel allégement.

ARTICLE 18

18. La documentation prévue au paragraphe 1° de l'article 17 doit au moins :

1° permettre d'identifier le document devant être transféré;

2° indiquer le procédé employé pour effectuer le transfert, lequel doit s'appuyer sur des normes ou standards techniques reconnus par un organisme de normalisation national ou international visé à l'article 69;

3° comporter un registre des dysfonctionnements survenus lors du transfert ainsi que des correctifs apportés pour y remédier;

4° être mise à jour pour tenir compte notamment des modifications qui peuvent être apportées au procédé de transfert, des inspections et des contrôles de sécurité effectués pendant la période où le document est sur le support récepteur;

5° être appuyée d'une déclaration de transfert par la personne qui l'a supervisé et qui atteste que l'autorisation de transfert a été accordée, que le procédé de transfert utilisé répond aux normes et a été fidèlement exécuté, que le document qui en a fait l'objet n'a pas été altéré au cours du transfert et que ces deux documents portent la même information.

> **La documentation et la déclaration sont jointes, directement ou par référence, soit au document résultant du transfert, soit à ses éléments structurants ou à son support. Elles sont conservées durant tout le cycle de vie de ce document.**

Nous réaffirmons, dans le contexte de cet article 18, qui établit une procédure relativement compliquée pour encadrer une opération informatique qui peut être très simple et rapide d'exécution, l'exclusion demandée ci-dessus pour les petites entreprises. Nous comprenons l'importance de documenter les transferts d'information dans le cas des fichiers de l'État ou des grandes entreprises. Nous doutons cependant fortement que des travailleurs autonomes ou autres petites entreprises documenterons d'une manière aussi exhaustive et procédurière les transferts de leurs fichiers vers un autre support. Il en résultera que bien peu de ces entités pourront aspirer à la fiabilité de leurs fichiers informatiques. La simple utilisation d'outils reconnus, comme pour le particulier, serait plus raisonnable et très certainement suffisante dans leur cas. Le ou les critères de distinction entre les entreprises soumises à ces articles rigoureux et celles qui en seront dispensées devront être établis avec soin afin de tenir compte par exemple de la possibilité que des renseignements personnels ou des dossiers médicaux soient détenus et manipulés par des petites entreprises. Des précautions devraient toujours être prises à l'égard de telles informations dont la fiabilité constante pourrait relever de la sécurité et de l'ordre public.

De façon générale, nous notons la lourdeur de la procédure imposée et l'impressionnante documentation exigée pour encadrer une opération que le niveau de technologie actuel rend plutôt simple. La conversion de fichiers informatiques se fait maintenant par quelques commandes et il ne faudrait pas qu'un processus aussi simple doive être entouré de procédures additionnelles beaucoup plus longues.

La solution réside peut-être dans la clarification de l'article 17 et de sa notion de « technologies différentes ». Si les conditions qui exigeront le respect des articles 17 et

suivants peuvent être suffisamment précisées et limitées, peut-être pourrons-nous éviter que des masses de documents technologiques perdent le niveau de fiabilité auquel ils ont droit.

ARTICLE 19

> **19. En cas de transfert vers le support papier, pour affirmer que le document papier porte la même information que le document technologique, afin que celui-ci puisse être détruit, la comparaison des deux documents doit être faite. Elle peut l'être soit sur place ou à distance, soit par un procédé approprié au support du document qui fait l'objet du transfert, soit par un examen visuel ou manuel des documents papier et technologique.**
>
> **De plus, la personne qui effectue le transfert doit faire mention du transfert sur le document qui en résulte et y joindre, directement ou par référence, une déclaration de transfert attestant que le document résultant du transfert porte la même information que le document qui en a fait l'objet.**

Cet article est lourd et n'apporte pas grand-chose. Nous suggérons donc de le retirer. Comme dans le cas des dispositions sur la copie certifiée, le critère de correspondance des contenus entre le document source et le résultat du transfert demeure. Que le transfert se fasse à partir ou vers le papier ne change rien. Répéter à nouveau ce principe alourdit inutilement l'avant-projet.

La description de la méthode à employer pour vérifier cette conformité des deux documents, par examen visuel ou manuel, à distance ou non, n'apporte rien non plus. Selon nous, la description des moyens à prendre ne relève pas vraiment d'un texte de loi.

Finalement, l'obligation de faire mention du transfert sur le document qui en résulte est redondant avec la même obligation qui découle de l'article 18, à notre avis suffisant à régler cette situation en biffant ses premiers mots : « ***Sauf dans le cas prévu à l'article 19 ».***

ARTICLE 25

> **25. L'intermédiaire qui offre des services de conservation de documents sur un réseau de communication n'est pas responsable des activités accomplies par l'utilisateur du service au moyen des documents conservés par ce dernier ou à la demande de celui-ci.**
>
> **Cependant, il peut devenir responsable s'il a de fait connaissance que les documents conservés servent à la réalisation d'une activité à caractère illicite ou s'il a connaissance de circonstances qui la rendent apparente et qu'il n'agit pas promptement pour rendre l'accès aux documents impossible ou pour autrement empêcher la poursuite de cette activité.**
>
> **De même, l'intermédiaire qui offre des services de référence à des documents, dont un index, des hyperliens, des répertoires ou des outils de recherche, n'est pas responsable des activités accomplies au moyen de ces services. Il peut le devenir, s'il a de fait connaissance que les services qu'il fournit servent à la réalisation d'une activité à caractère illicite et s'il ne cesse promptement de fournir ses services aux personnes qu'il sait être engagées dans cette activité.**

Nous soulignons une imprécision qui pourrait porter à confusion à l'alinéa 1 de cet article. Il mentionne en effet que l'intermédiaire n'est pas responsable des activités accomplies par l'utilisateur du service au moyen des documents ***« conservés par ce dernier »*** ou à sa demande. Nous croyons que l'article serait plus clair s'il utilisait le verbe « remisé », comme dans le document de travail préliminaire, plutôt que « conservé », puisque l'utilisateur ne conserve pas de documents, il les confie à l'intermédiaire qui, lui, les conserve sur son système.

Nous constatons, de façon plus générale, que l'avant-projet de loi traite, à différents endroits, de la responsabilité des intermédiaires. Chaque section se voyant ajouter un ou deux articles à ce sujet. Cette façon de faire n'est pas sans entraîner une certaine confusion et un éparpillement de ces dispositions capitales qui régissent un secteur du droit du cyberespace susceptible de faire l'objet de plusieurs actions devant les tribunaux. Nous notons aussi un certain flottement dans les termes utilisés dans chacun de ces articles, que ce soit dans la description de l'intermédiaire concerné ou dans les détails entourant ses obligations, la situation décrite ci-dessus étant assez représentative de ce problème. Systématiquement, le lecteur doit se demander quelle différence il peut y avoir entre deux dispositions, doit explorer les distinctions entre les types d'intermédiaires créés et procéder à une recherche exploratoire afin de découvrir d'autres articles qui pourraient s'appliquer à son cas. Cette situation se présente paradoxalement sur une toile de fond inspirée de ce qu'il est convenu d'appeler la « métaphore du libraire », selon laquelle l'intermédiaire n'est responsable qu'à partir du moment où il n'intervient pas après avoir eu connaissance d'un problème.

La complexité des dispositions, les variations dans leur rédaction, leur dissémination dans le texte et l'organisation générale de l'avant-projet de loi nous amènent à vous suggérer de rassembler en une seule section tous les articles concernant la responsabilité des intermédiaires et des autres intervenants. Nous sommes convaincus de plus que l'esprit de l'avant-projet de loi permettrait de cette manière de synthétiser encore mieux la situation, de réduire le nombre des articles traitant de ce sujet et d'éviter de très longs et compliqués débats jurisprudentiels pour les analyser. Le texte serait ainsi moins tortueux et la compréhension des niveaux de responsabilité des uns et des autres en serait, selon nous, grandement facilitée.

ARTICLE 29

> **29. Un prestataire de services à qui un document est confié est tenu, durant la période où il en a la garde, d'en assurer la sécurité, d'en préserver l'intégrité et, le cas échéant, d'en protéger la confidentialité et d'en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance.**
>
> **Il doit de plus assurer le respect de toute autre obligation prévue dans la loi relativement à la conservation du document.**

Nous constatons une certaine confusion dans les termes employés pour désigner la personne à qui un document est confié. Ainsi, à l'article 24, c'est l'expression « la personne chargée de la conservation d'un document technologique », à l'article 25, on utilise l'expression « l'intermédiaire qui offre des services », à l'article 29, il s'agit plutôt du « prestataire de services à qui un document est confié », à l'article 30, c'est « l'intermédiaire qui fournit les services ». À moins qu'on ait voulu distinguer différentes personnes en fonction du service fourni, il n'est pas aisé de comprendre les distinctions, car l'utilisation d'expressions aussi variées embrouille les lecteurs inutilement.

Par ailleurs, l'usage du terme très général « prestataire de services » à l'article 29 peut, selon nous, avoir des conséquences insoupçonnées. Ainsi, il n'est pas stipulé, à cet article, qu'il s'agit d'un prestataire de services de conservation de documents technologiques. Il se pourrait qu'il n'agisse qu'à une fin spécifique, tout à fait étrangère aux nouvelles technologies, par exemple, le comptable à qui nous pouvons transférer notre rapport d'impôt ou autres données sous forme électronique. Nous nous interrogeons sur l'intention qui motive cette disposition. S'il s'agit de prestataires de services en nouvelles technologies (hébergement, location d'espace-disque...), le terme devrait être remplacé afin d'éviter d'englober d'autres types de prestataires. Si, par ailleurs, il est de l'intention du législateur d'assurer la sécurité des documents

technologiques confiés à des tiers, l'usage du terme « prestataire de services » plutôt que, par exemple, « toute personne à qui un document est confié », vient limiter la portée de la disposition. Nous croyons cependant que nous pourrions, dans ce dernier cas, créer des obligations qui n'existent peut-être pas dans le monde réel. Ainsi, pour utiliser le même exemple, lorsque des documents sont confiés à un comptable, il est tenu d'en respecter la confidentialité de par ses obligations professionnelles générales. Le type de support utilisé (papier ou numérique) n'y change rien. Il devra prendre les mesures appropriées au support des documents reçus. Cependant, s'il confie des données comptables sur son entreprise à un acheteur éventuel, il devra lui faire signer une entente pour en protéger la sécurité, l'intégrité, etc. S'il ne le fait pas, il en assumera les conséquences. L'article 29 pourrait avoir pour effet d'imposer à l'acheteur potentiel des obligations légales si des informations au moyen d'un document technologique lui étaient transmises. Il y aurait là un changement aux règles usuelles du droit, et cela ne semble pas correspondre au but recherché par l'avant-projet de loi. Il y aurait lieu de s'interroger, si telle est l'intention du législateur, sur la pertinence d'élargir ainsi les obligations générales en matière de confidentialité.

ARTICLE 35

35. Lorsqu'une loi prévoit l'obligation de transmettre, d'envoyer, d'expédier ou de remettre à un même destinataire plusieurs exemplaires ou copies d'un document, cette obligation peut être satisfaite au moyen d'un seul exemplaire ou copie, lorsqu'il s'agit d'un document technologique.

Toutefois, l'expéditeur qui transmet plus d'un exemplaire ou copie doit être en mesure de vérifier l'intégrité des autres exemplaires ou copies générés, selon le cas, soit à partir de son système ou de celui du destinataire, soit en faisant appel à un document, y compris un logiciel, que le destinataire met à sa disposition.

> **De plus, lorsqu'un exemplaire ou une copie est généré par le destinataire, il doit de même en garantir l'intégrité.**

Concernant l'alinéa 2 de cet article, nous émettons certains doutes quant à la capacité pour l'expéditeur de vérifier l'intégrité des exemplaires ou copies générés par le système du destinataire. À compter du moment où le fichier a été transmis, l'expéditeur nous semble perdre tout contrôle, notamment en ce qui a trait à l'intégrité du document. Il nous apparaît plutôt que l'expéditeur, au moment de la transmission, doit s'assurer que les copies sont identiques et que sa responsabilité devrait s'arrêter là. Dès l'envoi, aucune autre responsabilité ne devrait lui être imposée. Le devoir de s'assurer de l'intégrité devrait incomber au destinataire qui a reçu les copies.

En conséquence, nous recommandons que l'alinéa 2 soit modifié comme suit :

> ***Toutefois, l'expéditeur qui transmet plus d'un exemplaire ou copie doit être en mesure de vérifier l'intégrité des autres exemplaires ou copies qu'il génère.***

De plus, le troisième alinéa apporte une certaine confusion générée par l'utilisation du pronom « il ». En effet, il est difficile de saisir si le « il » se rapporte à l'expéditeur ou au destinataire. En comparant la version de l'avant-projet de loi avec celle du document de travail qui nous avait été soumise, nous comprenons que c'est le destinataire qui est visé. D'ailleurs, il serait difficile pour l'expéditeur de faire les vérifications nécessaires en pareil cas. Mais, tous n'auront pas ce document en main quand ils voudront comprendre le sens de la loi. Il serait donc préférable de modifier cet alinéa comme suit :

> **De plus, lorsqu'un exemplaire ou une copie est généré par le destinataire, celui-ci doit en garantir l'intégrité.**

À cette ambiguïté, s'ajoute le fait que cet alinéa ne nous apparaît pas d'une grande utilité puisqu'il se contente de faire référence, encore une fois, au régime déjà encadré du

transfert d'information. La génération d'une copie par le destinataire du document technologique qu'il aura reçue, ne sera ainsi qu'un transfert d'information. Le destinataire qui y procédera devra s'assurer, conformément aux dispositions de l'avant-projet de loi sur le transfert d'information, que la nouvelle copie correspond à celle qu'il a reçue. Il n'y a pas lieu, selon nous, de répéter à nouveau ces obligations. Le dernier alinéa pourrait donc être retiré.

ARTICLE 36

> **36. Une présomption de fiabilité d'un document d'une entreprise au sens du Code civil ou en possession de l'État existe en faveur du particulier lorsque celui-ci en génère un exemplaire ou une copie à partir d'un système ou d'un document, y compris un logiciel, mis à sa disposition par l'un d'eux.**

À prime abord, l'usage du terme « particulier », dans cet article comme dans quelques autres, est quelque peu étonnant. Ce terme n'est généralement pas utilisé en droit civil, et sa définition pourrait être problématique. Nous aimerions beaucoup mieux que le terme « personne physique », qui correspond à une notion existante au *Code civil du Québec*, soit utilisée partout dans l'avant-projet de loi à la place du mot « particulier ».

Ensuite, nous vous avouons avoir du mal à saisir le motif ayant mené à cette discrimination en faveur du « particulier ». S'il l'on prévoit une présomption de fiabilité dans un tel contexte, ne devrait-elle pas bénéficier à toute personne et non pas seulement au particulier ? À titre d'exemple, le particulier qui obtiendrait un exemplaire d'un acte du RDPRM, organisme public, bénéficierait de cette présomption, mais le notaire (entreprise) non! Si nous admettons qu'à la base, une personne qui génère un document à partir d'un système mis en place par quelqu'un d'autre devrait être en mesure de s'y fier, cette disposition n'introduit-elle pas l'expression d'une certaine forme d'iniquité ?

Finalement, nous remarquons que l'article utilise deux termes « exemplaire » et « copie ». Nous ne voyons pas ce que l'usage de ces deux termes peut ajouter à l'article. Ainsi, dans le contexte de cet article, le document technologique existe déjà sur le système distant, et une tierce personne ne pourrait logiquement n'en générer qu'une copie. L'usage du terme « exemplaire », ainsi que la suggestion d'une distinction avec la notion de copie qui peut découler de cette rédaction, pourrait porter à confusion. Nous suggérons donc de n'utiliser que le terme « copie ».

En conséquence, nous recommandons que l'article 36 soit modifié comme suit :

> ***36. Une présomption de fiabilité d'un document émanant d'une entreprise ou en possession de l'État existe en faveur de toute personne lorsque celle-ci en génère une copie à partir d'un système ou d'un document, y compris un logiciel, mis à sa disposition par l'un d'eux.***

ARTICLE 37

> **37. Lorsque la loi déclare confidentiels des renseignements que comporte un document, leur confidentialité doit être protégée par un moyen approprié au mode de transmission, y compris sur des réseaux de communication ouverts ou fermés.**
>
> **La confidentialité du document transmis peut être protégée, entre autres par le chiffrement du document avant sa transmission, par l'utilisation de canaux de communication munis de fonctions de chiffrement, par l'utilisation de canaux de communication dont une personne est responsable et qui sont dédiés à la transmission de ses documents ou de ceux provenant de personnes à qui elle donne accès à ces canaux ou par tout autre moyen convenu entre l'expéditeur et le destinataire.**

> **La documentation expliquant le mode de transmission convenu doit être disponible pour production en preuve, le cas échéant.**

L'alinéa 2 n'a d'autre utilité, à notre sens, que de fournir des exemples de moyens de protection de la confidentialité. Nous considérons que de tels exemples n'ont pas leur place dans une loi. Cela d'autant plus qu'il est fort possible que dans peu de temps les moyens énoncés ne soient plus utilisés et soient remplacés par d'autres qui n'y seront pas énumérés. Il est inutile, quant à nous, de figer dans le temps des concepts technologiques qui ne cesseront d'évoluer. D'autant plus que l'usage du verbe « peut » au début de cet alinéa, fait en sorte que l'énumération ne cherche même pas à être exhaustive. Nous suggérons donc de retirer le deuxième alinéa.

Les alinéas 1 et 3 sont en tous points suffisants à créer l'obligation de protéger les renseignements confidentiels.

Nous devons ici saluer l'audace du législateur, qui choisit un moyen d'intervention d'avant-garde pour aider à l'encadrement de la vie privée sur le Web. Nous remarquons en effet que l'article 37 fait appel aux théories de Joel Reidenberg[7] et Lawrence Lessig[8], connues sous le vocable de « régulation par l'architecture ». L'application de solutions techniques aux problèmes issus de la technique, surtout par le biais d'articles généraux comme celui-ci pourrait bien permettre à nos systèmes juridiques de tirer profit de solutions et des protocoles de pointe mis en place pour assurer le respect des droits des individus sur un réseau mondial. Nous pensons notamment au projet P3P (Platform for Privacy Preferences, www.w3c.org/p3p). Nous ne pouvons que nous en réjouir.

[7] Notamment *The Use of Technology to Assure Internet Privacy : Adapting Labels and Filters for Data Protection*, Joel Reidenberg, http ://www.lex-electronica.org/articles/v3-2/reidenbe.html.
[8] Notamment Code and other laws of cyberspace. Lawrence Lessig, Basic Books; ISBN : 0465039138.

ARTICLE 38

> **38. La partie qui, pour effectuer une communication s'exprime sans le concours d'une personne physique par l'intermédiaire d'un document préprogrammé doit, sous peine d'inopposabilité de la communication, faire en sorte que le document fournisse les instructions nécessaires pour que l'autre partie puisse dans les meilleurs délais l'aviser d'une erreur commise ou disposer des moyens pour prévenir ou corriger une erreur pour qu'elle soit en mesure d'éviter l'obtention d'un produit ou d'un service dont elle ne veut pas ou qu'elle n'obtiendrait pas sans cette erreur ou pour qu'elle soit en mesure de le rendre ou, le cas échéant, de le détruire.**

La lourdeur de cet article est en soi suffisante pour demander qu'il soit réécrit. À cette occasion, il serait opportun d'éclaircir un fait. Qui ou quoi est à l'origine de l'erreur dont on parle ? Le logiciel, l'acheteur ? Est-ce une erreur technique ou humaine ou les deux ? Est-ce que cette « erreur » permet implicitement la faculté de dédit ? Nous voyons là que la notion d'erreur peut être interprétée très largement. Il serait donc préférable que lors de la nouvelle rédaction de cette disposition, des précisions soient apportées à cet égard. Par ailleurs, de devrait-on pas prévoir la nullité du contrat dans les cas prévus par cette disposition ?

La rédaction générale de cet article est inutilement compliquée. Par exemple, on pourrait simplement dire ***« La partie qui communique par l'intermédiaire d'un document préprogrammé doit... »*** au lieu de ***« La partie qui, pour effectuer une communication s'exprime sans le concours d'une personne physique par l'intermédiaire d'un document préprogrammé doit... »***

Aussi, la dernière partie de l'article « ***pour qu'elle soit en mesure d'éviter l'obtention d'un produit ou d'un service dont elle ne veut pas ou qu'elle n'obtiendrait pas sans cette erreur ou pour qu'elle soit en mesure de le rendre ou, le cas échéant, de le détruire*** » devrait être carrément supprimée. Elle n'ajoute rien et complique inutilement la compréhension de la disposition.

ARTICLES 39 ET 40

> **39. L'intermédiaire qui fournit les services d'un réseau de communication exclusivement pour la transmission de documents sur ce réseau n'est pas responsable des actions accomplies par autrui au moyen des documents qu'il transmet ou qu'il conserve durant le cours normal de la transmission et pendant le temps nécessaire pour en assurer l'efficacité.**
>
> **Il peut devenir responsable s'il est à l'origine de la transmission du document, s'il sélectionne ou modifie l'information du document, s'il sélectionne la personne qui le transmet ou qui le reçoit ou qui y a accès ou s'il conserve le document plus longtemps que nécessaire pour sa transmission ou s'il participe autrement à l'action d'autrui.**
>
> **40. L'intermédiaire qui, dans le cadre des services de transmission qu'il fournit sur un réseau de communication, conserve sur celui-ci les documents que lui fournit son client, à seule fin d'assurer l'efficacité de leur transmission ultérieure aux personne qui ont droit d'accès à l'information, n'est pas responsable des actions accomplies par autrui par le biais de ces documents.**
>
> **Il peut devenir responsable dans les cas visés au deuxième alinéa de l'article 39 ou s'il ne respecte pas les conditions d'accès au document, s'il prend des mesures pour empêcher la vérification de qui y a eu accès ou s'il ne retire pas promptement du réseau ou ne rend pas l'accès au document impossible alors qu'il a de fait**

connaissance qu'un tel document a été retiré de là où il se trouvait initialement sur le réseau, du fait qu'il n'est pas possible aux personnes qui y ont droit d'y avoir accès ou du fait qu'une autorité compétente en a ordonné le retrait du réseau ou en a interdit l'accès.

Nous réitérons ici notre conseil de regrouper toutes les dispositions portant sur la responsabilité des intermédiaires et de les refondre en quelques dispositions générales, à plus large portée et moins sujettes à interprétation.

LES MOYENS DE RELIER UNE PERSONNE ET UN DOCUMENT TECHNOLOGIQUE

ARTICLE 41

41. Le lien entre une personne et un document technologique peut être établi par tout procédé ou par une combinaison de moyens, dans la mesure où ils permettent :

1° de confirmer l'identité de la personne qui effectue la communication ainsi que son association au document et, au besoin, sa localisation;

2° d'identifier le document et, au besoin, sa provenance, son parcours et sa destination à un moment déterminé.

L'ajout de « ***ou par une combinaison de moyens »*** nous apparaît inutile, puisque cette possibilité serait comprise dans « ***par tout procédé*** ».

ARTICLE 44

44. Le système de cryptographie asymétrique peut permettre d'apposer une signature ou autrement servir à l'établissement d'un lien entre une personne et un document.

> **Dans ce système, la personne titulaire d'une biclé qui utilise sa clé privée pour signer ou déchiffrer un document est présumée être la personne à qui correspond la clé publique liée à cette clé privée et dont l'identité est indiquée au certificat ou selon le cas, au répertoire visés à la section III, à moins que la partie qui conteste ce fait n'établisse, par prépondérance de preuve, qu'au moment de la signature ou du déchiffrement, une autre personne a utilisé sans droit la clé privée de la personne ainsi identifiée, que la signature du titulaire de la clé publique a été usurpée ou que la confidentialité de la clé privée a été levée de quelque manière.**
>
> **La personne identifiée dans un certificat comme titulaire d'une biclé est présumée avoir un lien avec le document qui est signé ou déchiffré à l'aide de la clé privée liée de façon indissociable à la clé publique.**
>
> **Le prestataire de services de certification qui fait appel à ce système doit être en mesure de confirmer le lien entre la personne ou l'objet et la clé publique qui lui est attribuée.**

L'inopposabilité d'une transaction effectuée avec une biclé ne devrait être admise qu'au cas où la clé privée a été utilisée sans droit ou frauduleusement. Le premier alinéa ajoute subrepticement une troisième éventualité, aux conséquences potentiellement désastreuse : ***« la confidentialité de la clé privée a été levée de quelque manière*** ». Ainsi, le titulaire d'une biclé qui, dans le cadre de ses affaires, autorise un commettant à utiliser sa clé privée pour mener certaines affaires (y compris dans le cas de personnes morales), même s'il a pris les précautions nécessaires pour encadrer l'usage de la clé, pourrait voir certaines transactions légitimement réalisées par ce biais, contestées par l'autre partie sur la base que la « confidentialité a été levée de quelque manière ». Nous voyons là une contradiction avec les termes de l'article 62 al 2 qui stipule que :

> **« Le titulaire de la biclé doit ensuite assurer la confidentialité de la clé privée et toute utilisation de cette clé est présumée faite par lui, même si, dans le cas d'une personne morale, d'une société, d'une association ou de l'État, le titulaire a autorisé une autre personne à la détenir pour lui. » (nos soulignements)**

La sécurité des transactions électroniques exige une précision sur ce point. Quoi qu'il en soit, si la signature du titulaire a été usurpée ou que la confidentialité de sa clé a été levée sans son consentement, nous pouvons affirmer sans peine que la clé a été utilisée sans droit. Le plus comprend le moins. Nous suggérons donc que l'article se lise comme suit :

> (…)
>
> ***« à moins que la partie qui conteste ce fait n'établisse, par prépondérance de preuve, qu'au moment de la signature ou du déchiffrement, une autre personne a utilisé sans droit la clé privée de la personne ainsi identifiée. »***

L'IDENTIFICATION ET LE REPÉRAGE DES PERSONNES, DES DOCUMENTS ET DES AUTRES OBJETS SERVANT À LA COMMUNICATION

ARTICLE 45

> **45. La personne qui, après vérification, est en mesure de confirmer l'identité d'une personne peut le faire au moyen d'un document, entre autres un certificat, qui doit être fiable et les enregistrements confidentiels qu'il est susceptible de comporter doivent être protégés. Ce document peut être transmis sur tout support.**

> **La vérification de l'identité d'une personne peut se faire en se référant aux registres prévus au Code civil ou à la *Loi sur la publicité légale des entreprises individuelles, des sociétés et de personnes morales* (L.R.Q., chapitre P-45) lesquels établissent l'identité d'une personne quel que soit le support au moyen duquel elle communique. La vérification de l'identité d'une personne peut aussi être effectuée à partir de caractéristiques, connaissances ou objets qu'elle présente ou possède.**
>
> **Cette vérification, faite par une personne ou pour elle, peut être effectuée, sur place ou à distance, par constatation directe ou au moyen de documents fiables et qui peuvent être disponibles sur différents supports pour consultation sur place ou à distance.**

Les alinéas 2 et 3 n'ajoutent rien de nouveau à l'alinéa 1 de l'article 45. Nous ne voyons ces alinéas que comme une énumération didactique de moyens de vérification de l'identité prévue au premier alinéa. Ainsi, l'utilisation du verbe « pouvoir » nous indique en premier lieu que les procédures énumérées ne sont pas obligatoires. Par la suite, la généralité des dispositions suivantes « par une personne ou pour elle », « sur place ou à distance », etc., font en sorte de laisser toutes les options ouvertes au vérificateur sans créer aucune obligation ou règle de droit.

Nous jugeons qu'en de telles circonstances, mieux vaut retirer ces exemples et ne conserver que le premier alinéa qui est en soi complet. Le choix des modes de vérification de l'identité relèvera de la personne qui y procède et qui engagera sa responsabilité par son attestation.

ARTICLE 49

> **49. À moins qu'une loi le prévoit expressément, nul ne peut exiger que l'identité d'une personne soit établie au moyen d'un procédé ou d'un dispositif qui permet de la localiser en tout temps et en tout lieu ou qui porte atteinte à son intégrité physique.**

Nous croyons tout à fait essentiel de prévoir l'impossibilité d'exiger l'établissement de l'identité d'un individu au moyen de tels procédés. Cet article constituera une sauvegarde importante pour les droits individuels face à des technologies de plus en plus raffinées et potentiellement envahissantes. Aussi, nous nous opposerons avec vigueur à la possibilité qu'une loi puisse faire fi de cette règle générale et permette expressément que l'identité d'une personne soit établie au moyen d'un dispositif portant atteinte à son intégrité physique. Nous pourrions à la rigueur comprendre une exception à la règle quant à la localisation d'un individu en tout temps. Mais, l'interdiction de porter atteinte à son intégrité physique ne devrait souffrir d'aucune exception. Il s'agirait là, de toutes façons, d'une entorse extraordinaire aux Chartes des droits et libertés, entorse malvenue qui, à notre avis, ne pourrait en aucune occasion trouver une justification valable aux yeux de la population.

Une telle disposition, durant les premières années d'existence de la loi, ne serait utilisée, nous n'en doutons pas, qu'avec la plus grande parcimonie, mais pourrait, par la suite, faire l'objet d'abus indescriptibles.

Par ailleurs, le libellé de cet article signifie que, même en l'absence d'une loi, une personne pourrait accepter l'installation, sans qu'on l'ait exigé, d'un dispositif permettant de la localiser en tout temps bien qu'il porte atteinte à son intégrité physique. Encore une fois, en ce qui concerne la protection de l'intégrité physique d'une personne, nous jugeons que l'interdiction devrait constituer une règle d'ordre public à laquelle il serait complètement impossible de déroger. Nous craignons les abus de pouvoirs dans l'obtention d'un tel consentement, en milieu de travail par exemple. Nous souhaitons fortement que cet article soit modifié de manière à interdire à quiconque d'établir l'identité d'une personne par ces moyens et d'interdire à toute personne d'accepter que son identité soit ainsi établie.

Le seul droit que nous sommes prêts à concéder est celui, pour les autorités, d'adopter une loi aux termes de laquelle il serait possible, dans des circonstances exceptionnelles, d'utiliser un procédé permettant de localiser un criminel. Et là encore ce ne serait qu'après avoir fait la démonstration sans équivoque qu'il s'agit de la seule mesure permettant d'assurer la protection du public compte tenu des antécédents de la personne visée. Une telle règle relèverait ici de la localisation et non pas de la protection de l'intégrité physique.

ARTICLE 50

50. Nul ne peut exiger que la vérification ou la confirmation de l'identité d'une personne soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques.

Lorsque la personne consent expressément à ce que son identité soit ainsi établie, il ne peut être fait appel qu'au minimum de caractéristiques ou de mesures permettant de la relier à l'action qu'elle pose et qui comptent parmi celles qui ne peuvent être saisies sans qu'elle en ait connaissance.

Tout autre renseignement concernant cette personne et qui pourrait être découvert à partir des caractéristiques ou mesures saisies ne peut être utilisé à aucune autre fin que la vérification ou la confirmation de son identité. Un tel renseignement ne peut être communiqué qu'à la personne concernée et seulement à sa demande. De même, aucune décision à l'égard de cette personne et qui serait relative à autre chose qu'à l'établissement de son identité ne peut être prise en se fondant sur ces caractéristiques ou mesures.

> **Ces caractéristiques ou mesures ainsi que toute note les concernant doivent être détruites lorsque l'objet qui fonde la vérification ou la confirmation d'identité est accompli ou lorsque le motif qui la justifie n'existe plus.**
>
> **La création d'une banque de caractéristiques ou de mesures biométriques doit être divulguée à la Commission d'accès à l'information et celle-ci peut rendre toute ordonnance concernant cette banque afin d'en déterminer la confection, l'utilisation, la consultation et la conservation y compris l'archivage et la destruction des mesures ou caractéristiques prises pour établir l'identité d'une personne.**

Lorsque comparé à l'article 49, nous remarquons que l'article 50 ne stipule pas qu'il sera possible de déroger à ses termes par une Loi. Bien que nous sachions très bien que ce fait ne pourrait empêcher le législateur de procéder quand même à une telle exception législative, nous soulevons que le fait que l'article 50, qui traite exclusivement de protection de l'intégrité physique, ne prévoit pas une telle possibilité, renforce notre argument quant à l'article 49.

Concernant le dernier alinéa de cet article, nous considérons que la Commission d'accès à l'information devrait pouvoir exercer *a priori* son pouvoir sur toute création d'une banque de caractéristiques ou de mesures biométriques. La rédaction de cet alinéa laisse suggérer que la Commission ne pourrait qu'intervenir *a posteriori*, puisqu'on y lit que la création d'une telle banque doit être « divulguée » à la Commission, et non pas qu'elle doit être « autorisée » par elle. L'existence d'une telle banque ne devrait pas simplement être divulguée après sa création, mais devrait plutôt faire l'objet d'une analyse approfondie sur son opportunité et de recommandations sur les conditions qui devraient encadrer sa constitution, son maintien et son opération. Ce ne serait qu'après avoir procédé à cette analyse que la Commission pourrait accorder ou non le droit de créer une telle banque.

De plus, le pouvoir accordé à la Commission de rendre toute ordonnance devrait être obligatoire. Nous vous suggérons donc de remplacer le mot « peut » par « doit ». Il serait inquiétant que de telles banques existent sans que les mesures visant la confection, l'utilisation, la consultation, la conservation, l'archivage et la destruction des informations n'aient fait préalablement l'objet d'ordonnances.

Nous émettons le souhait que dans l'hypothèse où telle banque finisse par exister, qu'elle soit gérée par un organisme gouvernemental, redevable envers la population et seul à pouvoir s'assurer que les informations qui y seraient contenues fassent l'objet de toutes les mesures de protection possible.

Enfin, nous constatons que l'article 59 du document de travail, concernant le caractère public des deux dispositions précédentes, n'avait pas été repris dans l'avant-projet de loi. Est-ce à dire qu'elles ont perdu ce caractère ou, plutôt, qu'il s'infère de l'objet même qui est traité ?

ARTICLE 51

51. Lorsqu'un document utilisé pour effectuer une communication en réseau est conservé à des fins de preuve, son identifiant doit être conservé avec lui pendant toute la durée de vie du document par la personne qui est responsable du document.

L'identifiant doit être accessible au moyen d'un service de répertoire, dont une des fonctions est d'associer un identifiant à sa localisation. L'association entre un identifiant et un objet peut être garantie par un certificat lequel est lui-même accessible au moyen d'un service de répertoire qui peut être consulté par le public.

Un identifiant se compose d'un nom de référence distinct et non ambigu dans l'espace nominatif local où il est inscrit, ainsi que des extensions nécessaires pour joindre ce nom aux autres

> **dénominations qui permettent de le situer dans un espace nominatif universel.**
>
> **Pour permettre d'établir la provenance, le parcours ou la destination du document à un moment déterminé, les autres objets qui ont servi à effectuer la communication, comme les certificats de clés publiques, les algorithmes, les serveurs, les routeurs et les aiguilleurs, doivent pouvoir être identifiés et localisés, au moyen des identifiants alors attribués à chacun de ces objets.**

Que de beaux débats jurisprudentiels en perspective! Nous ne pouvons qu'imaginer plusieurs procureurs débattre pendant des heures sur le sens de la distinction entre ***espace nominatif local*** et ***espace nominatif universel.*** Voici donc de nouvelles règles au régime de la preuve des documents électroniques qui a déjà fait l'objet de quelques articles dans l'avant-projet de loi. Si nous comprenons l'importance de la conservation des certificats de clés publiques, l'obligation faite de conserver indéfiniment à des fins de preuve des informations sur les véhicules techniques de la communication (***les algorithmes, les serveurs, les routeurs et les aiguilleurs***) suscite des interrogations à trois niveaux :

- la possibilité technique de le faire;
- si la chose est possible, la facilité pour le commun des mortels de remplir cette obligation;
- l'utilité de le faire.

Ainsi, à moins qu'il puisse nous être démontré que cette information est automatiquement générée, journalisée, toujours conservée avec le document et qu'elle peut être rendue accessible en tout temps, nous croyons qu'une telle stipulation est dangereuse et est même contraire à l'esprit de l'avant-projet de loi. Or, ce n'est pas le cas. Cette information doit être récupérée peu de temps après une communication et sauvegardée manuellement. D'autant plus que l'évolution galopante

du Web, l'augmentation exponentielle du nombre de ses composantes techniques et leur remplacement incessant par des unités de plus en plus puissantes, font en sorte que le chemin pris aujourd'hui par un document dans une transmission électronique sera probablement complètement différent demain. Il est donc tout à fait illusoire de penser que ces informations seront systématiquement répertoriées et conservées. Aujourd'hui, plus de 500 millions de comptes courriel sont utilisés dans le monde. D'ici deux ou trois ans, il est prévu que les comptes utilisés par les seuls américains généreront un trafic de plus de 400 milliards de messages. Vouloir ainsi encadrer les échanges électroniques relève de l'utopie.

Nous devons garder à l'esprit que la communication au moyen de documents technologiques, particulièrement sur Internet, constitue maintenant une opération facile et banale qui fait partie de la vie quotidienne de millions de gens. Le fait d'imposer à des opérations simples par leur nature l'obligation de respecter des procédures préalables archi-complexes, stipulées dans des articles aussi inabordables et hermétiques que l'article 51 pour leur accorder un statut d'élément admissible en preuve, ne peut que faire en sorte de dénier de manière définitive toute valeur juridique aux documents électroniques, puisque personne ne pourra satisfaire à de telles conditions.

Nous nous questionnons de toutes manières sur l'utilité juridique de conserver des informations sur ce que nous pourrions appeler les véhicules techniques de la communication. Une communication sur Internet est toujours brisée en morceaux (paquets), qui peuvent emprunter des itinéraires différents pour se rendre à destination. L'important, ce principe se retrouve d'ailleurs à l'article 34 al 3, est de pouvoir prouver l'envoi et la réception du document. Nous ne croyons pas que la détermination de toutes les étapes de son périple puisse être suffisamment importante pour en faire une obligation générale à l'utilisation en preuve de documents technologiques ainsi que l'impose l'article 51. Ceci reviendrait à imposer à la recevabilité d'une lettre envoyée par courrier recommandé (dont l'expédition et la

réception peuvent a priori être prouvées), de conserver après l'envoi de la lettre des informations sur les boîtes aux lettres, les bureaux de postes, les centres de tri, les camions, les postiers et les facteurs qui ont joué un rôle dans son acheminement.

Nous ne suggérerons pas de nouvelle formulation pour cet article, la tâche serait trop ardue. Mais nous ferons tout de même les quelques commentaires suivants. Ainsi, la prémisse de l'article « ***Lorsqu'un document utilisé pour effectuer une communication en réseau*** » mériterait d'être précisée puisque les circonstances qu'elles vise sont loin d'être claires. Ensuite, tel que mentionné, les termes ***espace nominatif local*** et ***espace nominatif universel***, qui apparaissent pour une première fois dans l'avant-projet de loi et ne sont définis nulle part, sont très malheureux et ne peuvent que dérouter le lecteur.

LA CERTIFICATION

ARTICLE 54

> **54. Lorsque le certificat vise une personne morale, une société, une association ou l'État, il doit permettre d'identifier la personne physique qui, le cas échéant, détient la clé privée liée à la clé publique dont le certificat fait mention.**
>
> **De plus, le nom distinctif d'une personne physique peut être un pseudonyme, mais le certificat doit indiquer qu'il s'agit d'un pseudonyme. Les services de certification sont tenus de communiquer le nom de la personne à qui correspond le pseudonyme à toute personne légalement autorisée à obtenir ce renseignement.**

L'alinéa 2 de cet article soulève une question : quelles seront ces personnes légalement autorisées à obtenir ce renseignement ? Les différents ministères ? Les forces de l'ordre ? Les ordres professionnels ? Comme il s'agit là, pour les services de certification, d'une obligation à laquelle il ne semble pas possible de se soustraire, il

serait opportun que dans le cadre même de cette loi, il soit indiqué quelles lois obligent à une telle divulgation de renseignements, et qui bénéficie de ce pouvoir.

ARTICLE 55

> **55. Le répertoire qui a pour fonction d'identifier ou de localiser une personne ou un objet ou d'établir un lien entre une personne et un objet doit être constitué conformément aux normes ou standards reconnus par un organisme de normalisation national ou international visé à l'article 69.**
>
> **Le répertoire doit être accessible au public, soit directement ou au moyen d'un dispositif, soit à l'aide d'une procédure d'accès aux différents domaines d'un réseau susceptibles de confirmer la validité d'un identifiant, d'un certificat ou d'un autre renseignement qu'il comporte.**
>
> **Toutefois, le répertoire ne peut rendre public le motif pour lequel un certificat a pu être suspendu ou annulé.**

Lorsque cet article, dans son premier alinéa, précise que le répertoire a pour fonction d'identifier ou de « *localiser une personne* », fait-on référence aux personnes qui seront localisées en tout temps en vertu d'une loi, tel que prévu à l'article 49 ou s'agit-il, plus bêtement, d'un simple répertoire d'adresses ? L'usage du terme « localiser » comme description d'une fonction d'un répertoire semble donc un peu bizarre dans ce contexte.

ARTICLES 58 ET 59

> **58. Le prestataire de services de certification peut adhérer à un régime d'accréditation volontaire. L'accréditation est accordée par une personne ou un organisme désigné par le gouvernement. La procédure et les conditions d'octroi, les délais d'obtention, la modification des conditions d'accréditation, le renouvellement, la suspension ou l'annulation de l'accréditation, ainsi que les frais afférents, sont établis par règlement du gouvernement.**
>
> **Les mêmes critères sont appliqués quelle que soit l'origine territoriale du prestataire. L'accréditation fait présumer que les certificats délivrés par le prestataire répondent aux exigences de la présente loi.**
>
> **59. Les certificats délivrés par un prestataire de services de certification en fonction d'autres normes que celles applicables au Québec peuvent être considérés équivalents aux certificats délivrés par un prestataire de services de certification accrédité. L'équivalence doit être constatée par la personne ou l'organisme désigné par le gouvernement pour conclure des ententes de reconnaissance mutuelle de tels certificats avec l'autorité désignée qui a établi ces normes. Il en est de même pour les services de répertoire.**
>
> **Les prestataires accrédités ou dont les services sont reconnus équivalents à ceux d'un prestataire accrédité doivent être inscrits dans un registre accessible au public par la personne ou l'organisme qui a constaté l'équivalence.**

Le seul commentaire que nous formulons concernant ces deux articles est le suivant : « la personne ou l'organisme désigné par le gouvernement » dont on parle, sera-t-il le même dans les deux cas ? S'agira-t-il d'une seule personne ou d'un seul organisme ou

y aura-t-il autant de personnes ou d'organismes que le gouvernement le souhaitera ? Nous sommes d'avis que ce devrait être la même personne ou le même organisme.

ARTICLE 60

> **60. Pour la délivrance ou le renouvellement d'une accréditation, il est tenu compte, outre l'information contenue dans l'énoncé de politique proposé, au moins :**
>
> **1. du fait que l'identité de la personne qui fait la demande est établie;**
>
> **2. de l'étendue de l'expertise, de l'infrastructure mise en place, des services offerts ainsi que de la disponibilité de garanties financières pour exercer l'activité;**
>
> **3. des garanties d'intégrité, d'accessibilité et de sécurité des répertoires ou des certificats fournis;**
>
> **4. des garanties d'intégrité, d'accessibilité et de sécurité des répertoires ou des certificats fournis;**
>
> **5. de l'applicabilité des politiques énoncées et, en cas de renouvellement, de leur application ainsi que du respect des autres obligations qui incombent à un prestataire de services.**

Nous vous avons déjà fait part de l'intérêt pour la Chambre des notaires du Québec et ses membres de prendre part, dans la mesure de leurs compétences respectives, aux services reliés à la certification d'identité. Les 3 200 notaires, dispersés à travers le Québec, ont une longue habitude de la vérification d'identité puisque leur loi organique leur impose un devoir en ce sens, lequel est repris au *Code civil du Québec*.

Quant à la Chambre des notaires, elle possède l'expertise souhaitée sur le plan de la gestion d'un registre. En effet, la Chambre tient avec le plus grand succès depuis 1961

le registre des testaments. Depuis cette date jusqu'au 1er janvier 2000, 4 463 719 testaments ont été inscrits et 419 452 certificats de recherches ont été émis. Le registre des mandats donnés en prévision de l'inaptitude du mandant existe, quant à lui, depuis 1991 et 649 951 mandats ont été inscrits, tandis que 4190 certificats de recherche ont été délivrés.

La Chambre des notaires mène depuis 1997 des travaux d'envergure qui lui permettent de tirer profit des technologies de pointe les plus récentes dans la tenue et l'exploitation de ces registres au grand avantage du public. Ces travaux ont notamment pour effet de permettre aux notaires de faire parvenir leurs avis des testaments et des mandats par voie électronique en utilisant leur signature numérique, lesquels avis sont automatiquement transférés dans la base de données.

Ainsi, la Chambre des notaires, tout comme ses membres, s'intéresse de très près aux travaux qui seront menés relativement à la certification d'identité et aux services de certification et de répertoire, afin d'y jouer éventuellement un rôle actif.

Cependant, nous ne souhaitons pas, dans le cadre de cette analyse des articles de l'avant-projet de loi, élaborer davantage sur cette question. Nous avons néanmoins préparé un document sur le sujet qui vous est présenté en annexe.

ARTICLE 61

61. Le prestataire de services de certification doit présenter des garanties d'impartialité par rapport à la personne ou l'objet visé par la certification, même s'il n'est pas un tiers à leur égard.

Il doit assurer la fiabilité des certificats qu'il délivre au cours de tout le cycle de vie du certificat, y compris en cas de modification, de suspension, d'annulation ou d'archivage du certificat ou de mise à jour d'un renseignement qu'il contient.

La formulation de l'alinéa 1 porte à confusion. Nous vous proposons de le modifier afin que nous puissions comprendre d'emblée que le prestataire doit présenter des garanties d'impartialité par rapport à la personne visée par la certification ***surtout*** s'il n'est pas un tiers à son égard. Ne va-t-il pas de soi que cette garantie d'impartialité est forcément assurée lorsqu'il *est* un tiers à son égard ?

ARTICLE 62

> **62. Lorsque la certification vise le titulaire d'une biclé dans un système de cryptographie asymétrique, la personne qui génère la biclé permettant la signature d'un document doit remettre, au titulaire de cette biclé, la clé privée qui la compose, de manière que seul ce dernier reçoive l'information secrète qu'elle contient.**
>
> **Le titulaire de la biclé doit ensuite assurer la confidentialité de la clé privée et toute utilisation de cette clé est présumée faite par lui, même si, dans le cas d'une personne morale, d'une société, d'une association ou de l'État, le titulaire a autorisé une autre personne à la détenir pour lui.**
>
> **En cas de perte ou de vol de la clé privée ou si le titulaire ou le détenteur de la biclé a des motifs raisonnables de croire que la confidentialité de la clé privée est compromise, il doit aviser, dans les meilleurs délais, le prestataire de services de certification pour que celui-ci puisse suspendre ou annuler le certificat de clé publique. Lorsque le détenteur de la clé privée n'est pas le titulaire du certificat, il doit aviser ce titulaire.**
>
> **Il est interdit d'utiliser une clé privée pour signer un document sachant que le certificat de clé publique correspondant est suspendu ou annulé.**

Encore ici, l'usage du terme « même si » laisse perplexe (al 2 : ***même si dans le cas d'une personne morale, d'une société, d'une association ou de l'État, le titulaire a autorisé une autre***

personne à la détenir pour lui). Ainsi, nous nous demandons si cette dernière partie de l'alinéa 2, qui n'apparaissait pas à l'article 71 du document de travail, vient simplement confirmer que les modes de gestion des clés privées au sein de ces entités particulières ne limite pas la présomption d'usage par le titulaire de la clé ou si, par surcroît, elle vient plutôt légitimer la délégation dans l'usage des clés privées en restreignant, a contrario, cette pratique à ceux qui ne sont pas mentionnés après ce fameux « même si ». Cette question de la délégation permise ou non dans l'usage d'une clé privée devient alors plutôt confuse et il est dès lors assez ardu de comprendre clairement qui, aux termes de l'avant-projet de loi, peut déléguer l'usage de sa clé privée. Cet alinéa devrait, pour être clair, s'arrêter avant ce « même si ». Si le législateur souhaite permettre ou non la délégation des clés privées, ou les encadrer dans certaines circonstances, il devrait le faire par le biais d'un article dédié à ce sujet, qui serait clairement écrit. Cette question peut porter à conséquences et mérite que l'on s'y attarde.

ARTICLE 63

> **63. Celui qui fournit des renseignements afin d'obtenir pour lui-même la délivrance d'un certificat est tenu d'informer le prestataire de services de certification, dans les meilleurs délais, de toute modification de ces renseignements.**
>
> **Lorsque les renseignements sont fournis dans le cadre d'un mandat ou d'un contrat de service ou d'entreprise, celui pour qui le certificat a été délivré est tenu, subséquemment, de la même obligation d'information envers le prestataire de services.**

Dans le premier alinéa, il est question du « ***prestataire de services de certification »*** et dans le second du « ***prestataire de services »***. Celui dont on parle dans le deuxième est-il ce même prestataire ?

De plus, nous nous interrogeons sur l'utilité du deuxième alinéa. Nous comprenons qu'il cherche à obliger la personne ayant bénéficié d'un service de certification par le biais

cette fois d'un intermédiaire, à fournir les informations requises à la tenue de son dossier à jour. Le premier alinéa ne précisant pas à qui les renseignements initiaux ont été fournis, nous croyons que l'éventualité où un intermédiaire agirait entre le « client » et le prestataire de services de certification se trouve comprise dans l'obligation générale. Selon nous, le deuxième alinéa n'ajoute rien et pourrait donc être retiré. À moins qu'il ne serve un autre objet qui aurait alors avantage à être précisé.

ARTICLE 64

> **64. Dans le cadre d'une communication au moyen d'un document technologique, la validité et la portée du certificat doivent être vérifiées avant de se fonder sur lui pour obtenir confirmation de l'identité de toute partie à la communication ou de l'exactitude d'un identifiant d'un objet.**
>
> **De même, avant de se fonder sur un renseignement inscrit au certificat, il faut vérifier si le prestataire de services de certification confirme l'exactitude du renseignement.**
>
> **La vérification peut être faite au répertoire ou à l'emplacement qui y est indiqué ou auprès du prestataire, au moyen d'un dispositif de consultation sur place ou à distance.**

Nous avons le sentiment, en lisant cette disposition, que le législateur a voulu expliquer aux utilisateurs les différentes étapes d'un processus, un peu comme si on nous fournissait un extrait d'un manuel d'instructions. L'article 64 viserait donc à expliquer ce qu'il faut faire avec un certificat. Il s'agit d'un article didactique qui ne trouve pas sa place dans une loi et qui peut avoir un effet pernicieux en introduisant une obligation de vérification du certificat. Et il est très probable que cette obligation ne sera pas respectée. L'on comprend que cette situation pourrait fournir une échappatoire aux autorités de certification qui n'auraient qu'à démontrer que le tiers n'a pas vérifié la validité et la portée du certificat, au détriment du tiers de bonne foi qui s'est fié sur le

certificat. Nous recommandons, en conséquence, de retirer cette disposition de l'avant-projet de loi.

ARTICLE 65

> **65. Les prestataires de services de certification et de répertoire et les personnes visées aux articles 62 à 64 ne sont tenues qu'à une obligation de moyens.**
>
> **À moins qu'ils puissent se dégager de leur responsabilité, ils sont tenus conjointement de réparer tout préjudice résultant de la communication en raison de l'inexactitude ou de l'invalidité du certificat ou d'un renseignement contenu au répertoire. Toutefois, en l'absence de faute de leur part, la réparation du préjudice est assumée à parts égales par ceux-ci.**
>
> **Nul ne peut exclure la responsabilité qui lui incombe en vertu du présent article.**

En toute honnêteté, nous avons cherché activement à comprendre le sens de cet article, mais en vain. La manière dont cette disposition est rédigée laisse entendre que si le prestataire ne peut se dégager de sa responsabilité, il est tenu conjointement et, par ailleurs, en l'absence de faute de sa part, il répare le préjudice pour partie. Est-ce que ça ne veut pas dire la même chose, soit : même s'il n'a commis aucune faute, il paie sa part ? Nous vous avouons être quelque peu perplexes devant cette formulation, mais peut-être avons-nous mal compris ?

De plus, comment prétendre qu'ils ne sont tenus qu'à une obligation de moyens - soit dit en passant, pourquoi l'avoir rédigé en forme négative ? - si on leur impose, de toute façon, de réparer le préjudice pour leur part ? Ne serait-il pas plus logique et conséquent de prévoir qu'en l'absence de faute, le prestataire n'est pas tenu de réparer ni en totalité ni en partie, le préjudice ? Nous croyons, quant à nous, que c'est la voie à

retenir dans ce contexte particulier, autrement il s'agirait là d'une responsabilité exorbitante pour le prestataire de services non fautif.

ARTICLE 66

> **66. Constitue une fausse représentation le fait de délivrer un document présenté comme étant un certificat confirmant l'identité d'une personne ou l'exactitude d'un identifiant d'un objet, alors qu'aucune vérification n'est faite par le prestataire de services ou pour lui ou que l'insuffisance de la vérification effectuée équivaut à une absence de vérification.**

L'utilité de cet article nous échappe. Il nous apparaît qu'il ne fait que qualifier une activité du vocable de « fausse représentation ». Aucune sanction n'est rattachée à cette désignation. Cette disposition semble parachutée, d'autant plus que cette notion de « fausse représentation » n'apparaît nulle part ailleurs dans l'avant-projet de loi. Il y aurait lieu de développer quelque peu la conséquence rattachée à un tel comportement ou de retirer cette disposition.

ARTICLE 67

> **67. Pour favoriser l'harmonisation des systèmes, des normes et des standards techniques mis en place pour la réalisation des objets de la présente loi, le gouvernement peut constituer un comité multidisciplinaire composé de membres, dont un président, qu'il choisit après consultation du milieu des affaires, de l'industrie des technologies de l'information et de la recherche scientifique et technique ainsi que de représentants des secteurs public et parapublic.**
>
> **Le président doit être un membre du Bureau de normalisation du Québec. Le comité peut faire appel à d'autres personnes possédant une expertise relative au domaine des technologies de l'information.**

> **Les membres du comité ne sont pas rémunérés, sauf dans les cas, aux conditions et dans la mesure que peut déterminer le gouvernement. Ils ont cependant droit au remboursement des dépenses faites dans l'exercice de leurs fonctions, aux conditions et dans la mesure que détermine le gouvernement.**

Nous notons tout d'abord l'absence de représentants du milieu juridique dans l'énumération des membres du comité. Or, ce comité recherchera l'harmonisation des systèmes mis en place pour réaliser les objets de la loi. Ces objectifs étant principalement constitués de notions de droit, la présence sur ce comité de représentants des professions juridiques, plus particulièrement de juristes versés en droit des nouvelles technologies de l'information nous apparaît tout à fait incontournable si ce comité doit formuler des conclusions d'ordre légal. De plus, vu l'importance de ce comité et son rôle déterminant, nous sommes d'avis que le texte devrait être corrigé afin de remplacer le mot ***peut*** créer ce comité par le mot ***doit*** créer ce comité.

L'alinéa 3 ne nous apparaît pas vraiment relever d'un texte législatif. D'ailleurs, il est loin d'assurer le caractère gratuit de la participation des membres de ce comité.

Ensuite, nous remarquons la disparition dans l'avant-projet de loi, du deuxième comité qui était prévu au document de travail. Ce « comité de concertation » nous semblait pourtant très prometteur, et peut-être même plus important que le comité multidisciplinaire, de par l'implication qu'il offrait aux intervenants des différents milieux de la société. La révolution technologique touche tout le monde et nous aimions l'idée de la création d'un forum où les problèmes découlant de leurs applications les plus sérieuses auraient pu être débattus. Nous déplorons donc cette mort subite du comité de concertation.

ARTICLE 70

> **70. La notion de document prévue par la présente loi s'applique à l'ensemble des documents visés dans les textes législatifs que ceux-ci y réfèrent par l'emploi du terme document ou d'autres termes notamment, acte, annales, annexe, annuaire, arrêté en conseil, billet, bottin, brevet, bulletin, cahier, carte, catalogue, certificat, charte, constat d'infraction, décret, dépliant, dessin, diagramme, écrit, électrocardiogramme, enregistrement sonore, magnétoscopique ou informatisé, facture, fiche, film formulaire, graphique, guide, illustration, imprimé, journal, livre, livret, logiciel, manuscrit, maquette, microfiche, microfilm, note, notice, pamphlet, parchemin, pièce, photographie, procès-verbal, programme, prospectus, rapport, rapport d'infraction et recueil.**
>
> **Dans la présente loi, les règles relatives au document peuvent, selon le contexte, s'appliquer à l'extrait d'un document ou à un ensemble de documents.**
>
> **Un dossier peut être composé d'un ou de plusieurs documents.**

Jusqu'ici l'avant-projet de loi traitait du document et, parfois, de banque de données. Mais, jamais avant l'article 70 n'avait-on introduit la notion de « dossier ». Nous nous interrogeons donc sur le sens qu'il faut lui donner. Nous avions retenu des articles 3 et 4 de l'avant-projet qu'une banque de données pouvait être assimilée au document et que celui-ci, même fragmenté, formait un tout et, inversement, que plusieurs documents réunis conservaient leur caractère distinct. Dans ce contexte, quelle est l'utilité du dossier, si à ces articles 3 et 4, le législateur n'a pas pris la peine d'en parler ? L'introduction de cette notion, absente du reste du projet, ne peut-elle pas confondre le lecteur ?

Quant à l'énumération de l'alinéa 1, nous la trouvons plutôt déroutante. Nous nous questionnons aussi sur son utilité, puisque l'usage du « notamment » fait en sorte qu'elle n'est même pas limitative. Nous comprenons par ailleurs l'importance, en vertu du principe des équivalences, de stipuler que les termes similaires utilisés dans d'autres lois sont assimilés au « *document* » de l'avant-projet de loi. Cependant, l'énumération devrait, selon nous, être allégée en ne conservant que les termes les plus importants ou qui peuvent le plus porter à conséquence (comme acte, constat d'infraction, écrit …) ou remplacée par une disposition générale comme «…*selon que le contexte l'exige* » autrement dit en énonçant une règle générale permettant aux lecteurs d'induire par eux-mêmes que chacun des mots apparaissant dans cet article correspond à un document au sens de la loi. Cette solution serait plus simple et éviterait l'énumération fastidieuse de l'article 70.

ARTICLE 71

> **71. Le paragraphe 1 du premier alinéa de l'article 11 s'applique lorsque sont employés, dans les textes législatifs, les termes « double », « duplicata », « exemplaire original » et « triplicata » et que le contexte indique que le document auquel ils réfèrent doit avoir une valeur d'original en tant que source première d'une reproduction.**

Nous nous interrogeons sur la décision de placer cette disposition à l'article 71, pour simplement faire un renvoi à l'article 11. Nous croyons qu'il serait plus simple d'intégrer cette règle directement dans l'article 11.

ARTICLE 73

> **73. L'indication, dans une loi, de modes de transmission comme l'envoi ou l'expédition d'un document par le courrier, par lettre, par la poste, par messager, par câblogramme ou télégramme, par télécopieur, par voie télématique, informatique ou électronique, par voie de télécommunication, de télétransmission ou au moyen de la fibre optique ou d'une autre technologie de l'information et ce, sur des réseaux de communication ouverts ou fermés n'empêche pas de recourir à un autre mode de transmission approprié au support du document comme prévu à l'article 31.**

L'article 31 prévoit l'usage d'un mode de transmission approprié au support du document, sauf si un mode particulier est exigé par la loi. L'article 73 mentionne que si une autre loi stipule un mode particulier de transmission, les modes de l'article 31 peuvent être utilisés. N'y a-t-il pas contradiction ? Comment sortir de cette boucle ?

ARTICLE 74

> **74. Lorsqu'une loi prévoit qu'une signature peut être gravée ou imprimée ou apposée au moyen d'un fac-similé gravé, imprimé ou lithographié ou qu'une marque peut l'être au moyen d'une griffe, d'un appareil ou d'un procédé mécanique ou automatique, elle doit être interprétée comme permettant, sur support papier, d'apposer la signature autrement que de façon manuscrite ou de faire apposer la marque personnelle par quelqu'un d'autre. Une telle disposition n'empêche pas de recourir à un autre mode de signature approprié à un document, lorsque ce dernier n'est pas sur support papier.**

Nous croyons qu'il va de soi que si une loi prévoit l'utilisation d'une signature gravée, elle permet la signature autre que manuscrite. Devons-nous créer une règle pour confirmer l'évidence ? La dernière phrase de l'article est cependant importante et devrait demeurer. L'article pourrait se lire simplement comme suit :

74. Lorsqu'une loi prévoit qu'une signature peut être gravée ou imprimée ou apposée au moyen d'un fac-similé gravé, imprimé ou lithographié ou qu'une marque peut l'être au moyen d'une griffe, d'un appareil ou d'un procédé mécanique ou automatique, elle doit être interprétée comme n'empêchant pas de recourir à un autre mode de signature approprié à un document, lorsque ce dernier n'est pas sur support papier.

ARTICLE 75

75. Une disposition créatrice d'infraction qui prévoit que celle-ci peut être commise au moyen d'un document doit être interprétée comme indiquant que l'infraction est commise, que ce document soit, à quelque moment de son cycle de vie, sur support papier ou sur un autre support.

Une petite erreur semble s'être glissée dans cette disposition. L'énoncé selon lequel « *une disposition créatrice d'infraction qui prévoit que celle-ci* ***peut être*** *commise au moyen d'un document, elle doit être interprétée comme indiquant que l'infraction* ***est*** *commise*, devrait, dans ce contexte être remplacé par « *elle doit être interprétée comme indiquant que l'infraction* ***peut être*** *commise* », plutôt que par ***est*** *commise.* Cela apparaîtrait plus logique.

CONCLUSION

Cette société où les technologies de l'information joueront un rôle prédominant dans toutes les sphères de la vie des citoyens est à deux pas, deux minutes, de nous. Certains la souhaitent ardemment, car ils l'imaginent et la conçoivent telle qu'elle sera, d'autres y aspirent parce qu'ils sont ceux qui en tissent l'écheveau, tandis que les derniers, la majorité, sont partagés entre la fascination et la crainte. Cette société est déjà en place et bien qu'elle mérite quelques ajustements ou raffinements, elle est là à nos portes et même, pour un certain nombre d'entre nous, déjà confortablement installée à l'intérieur de nos foyers. L'avant-projet de loi que vous avez présenté est l'expression même du progrès de ce mouvement.

Nous ne pouvons qu'approuver sans réticence les objectifs de cet avant-projet de loi. De notre côté, nous consacrons tous nos efforts pour permettre au notariat d'être à l'avant-garde dans l'utilisation des technologies de l'information afin que tous les notaires du Québec puissent, de toutes les manières, en tirer profit tout en assurant à la population qu'ils desservent des garanties de sécurité. Le projet de révision de la *Loi sur le notariat* a d'ailleurs été conçu dans cette optique.

Aussi, en dépit des critiques formulées tout au long de notre mémoire, lesquelles n'avaient d'autres visées que de porter à votre attention des suggestions visant soit à améliorer des dispositions, soit à éclairer les lecteurs sur certains points, nous apprécions à sa juste valeur le travail extraordinaire du ministre délégué à l'Autoroute de l'information et aux services gouvernementaux, M. David Cliche et à son équipe.

La Chambre des notaires remercie donc les membres de cette Commission d'avoir pris connaissance du présent mémoire et de lui avoir permis de le présenter. La Chambre est toujours heureuse de participer à l'élaboration des lois du Québec, notamment quand elles touchent l'ensemble des citoyens comme le fera sans nul doute la *Loi sur la normalisation juridique des nouvelles technologies de l'information*.

ANNEXE

Annexe

Commentaires généraux sur le chapitre III de l'avant-projet de loi, *Loi sur la normalisation juridique des nouvelles technologies de l'information*

Présentation de la question

Tel que précisé dans les notes explicatives l'accompagnant, l'avant-projet de loi en titre a notamment pour objet d'assurer la sécurité juridique des communications effectuées au moyen des nouvelles technologies de l'information. À cet effet, l'avant-projet de loi, à son chapitre III, établit des normes qui tendent à garantir l'identification d'une personne ainsi que le lien qui existe entre cette personne et un document technologique donné.

L'application de ces normes passe bien entendu par des procédés purement technologiques, mais aussi par des services de certification et de répertoire. Aux termes de l'article 56, ces services peuvent être offerts par une personne ou par l'État. Le notariat québécois considère être le candidat idéal pour offrir de tels services de certification et de répertoire et il entend en faire ci-après la démonstration.

Comme le Gouvernement, la Chambre des notaires du Québec estime que la vérification de l'identité d'une personne au moyen d'un certificat est essentielle à la protection des communications réalisées avec les nouvelles technologies de l'information. En effet, « la dématérialisation des transactions amplifie le risque qu'une personne transige sous une identité fictive ou usurpe l'identité d'une autre personne »[1]. La vérification de l'identité d'une personne sert donc à prévenir ces cas de dol. Pour atteindre cet objectif, certaines mesures de sécurité doivent être mises en place. Des normes trop lâches, tout comme une application sans rigueur de mesures plus strictes

auraient rapidement pour effet de multiplier les cas de fraude. Celle-ci s'avérerait alors d'autant plus dévastatrice que le consommateur s'en croirait à l'abri sous la protection de la Loi. Ainsi, faut-il exclure toute forme « d'auto-vérification » et tout procédé de vérification à distance. Pour être valable, sûre et respectueuse de la personne, la vérification d'identité devra être réalisée par un tiers en la présence physique du demandeur.

Cette exigence n'exclurait pas cependant une certaine modulation du niveau de sécurité. Cette modulation se ferait en fonction des objectifs transactionnels recherchés par rapport aux coûts économiques inhérents aux différents niveaux de vérification disponibles. Par exemple, la procédure pourrait être moins élaborée, et par conséquent moins coûteuse, pour certains types d'échanges de consommation courante que pour d'autres où des enjeux importants de protection des cocontractants ou de respect de la vie privée seraient en cause. L'utilisation d'une signature numérique donnée dépendrait donc des limites prévues au certificat y correspondant.

Pour maintenir le niveau de sécurité recherché : « Il va sans dire que les autorités de certification choisies devront présenter des garanties d'intégrité et d'impartialité suffisantes. Il importe également que les utilisateurs manifestent une confiance quasi absolue envers cet organisme, qu'il soit public ou privé, de façon que l'infrastructure de certification soit exploitée au maximum »[2].

Les caractères fondamentaux du notariat

Depuis toujours[3], le notaire a le devoir de vérifier l'identité des parties dont il reçoit la signature[4]. Il a l'obligation de conserver à son dossier la preuve de cette vérification et des pouvoirs d'agir de toute partie à un acte[5]. Il est également responsable d'assurer l'origine et l'intégrité des informations contenues à un acte qu'il a reçu et de conserver ce dernier reçu en minute[6]. Il doit maintenir le secret de tous renseignements confidentiels et veiller à ce que ses employés ne les communiquent à autrui[7]. Il se doit aussi d'observer les règles de la probité et de l'impartialité la plus scrupuleuse[8].

La Chambre des notaires, dont la mission principale est la protection du public[9], vérifie régulièrement, au moyen d'inspections professionnelles rigoureuses, que les notaires se conforment à toutes ces obligations. D'ailleurs, les notaires en assument la responsabilité, non seulement à l'égard de leur Ordre professionnel, mais aussi face à leurs clients et aux tiers lésés par un éventuel manquement de leur part. Ces derniers sont protégés par l'assurance-responsabilité professionnelle obligatoire des notaires[10].

En contrepartie de ces obligations — et de bien d'autres — le notaire est reconnu comme officier public et les actes qu'il reçoit se voient accorder le privilège de l'authenticité[11]. « En effet, le notaire est un officier public, impartial et indépendant, investi d'une partie des pouvoirs de l'autorité publique lui ayant été délégués législativement par le gouvernement québécois, ayant le pouvoir et l'obligation de certifier sous sa responsabilité professionnelle le statut légal des parties à un acte juridique »[12].

En droit québécois, le notaire est « le seul mandaté par une loi particulière à conférer l'authenticité aux actes privés »[13]. Ses actes et les copies de tels actes bénéficient de la force probante qui s'attache aux actes de l'autorité publique[14]. En 1995, le Législateur a d'ailleurs réaffirmé les qualités intrinsèques de l'acte notarié, en amendant l'article 2993 du *Code civil du Québec*. Cet article reconnaît maintenant le caractère unique de l'acte notarié en précisant que l'apposition par un notaire de sa signature comporte notamment, en elle-même, l'attestation de l'identité d'une personne à un acte, aux fins de publication au registre foncier.

Le notaire bénéficie d'une crédibilité peu commune dans la population. Selon le dernier sondage *Léger & Léger* réalisé en août 1997, 91% des répondants ayant consulté un notaire se sont dits satisfaits des services obtenus. De plus, le notariat représente la profession juridique qui côtoie le plus large bassin de population puisque plus de 43% des répondants au sondage ont confirmé avoir consulté un notaire au cours des cinq dernières années. Ce sondage mesurait également le taux de confiance de la

population à l'égard des professions juridiques. À ce chapitre, les notaires se classaient bons premiers.

Le cadre législatif, réglementaire et disciplinaire de la pratique notariale conjugué au professionnalisme éprouvé du notaire et à la reconnaissance de ses qualités par la population ont permis d'assurer une sécurité du plus haut niveau dans les relations contractuelles au Québec. L'officier public qu'est le notaire, aidé dans sa tâche par le caractère authentique des actes qu'il reçoit, représente donc le meilleur spécialiste de la sécurité juridique.

L'évolution sociale et technologique

Se fondant sur ses caractéristiques fondamentales qui continuent d'être recherchées malgré les changements sociologiques et technologiques, le notariat québécois a maintes fois prouvé qu'il pouvait non seulement s'adapter aux nouvelles réalités, mais également les prévoir et se préparer avec sérieux à leur venue afin de mieux servir l'ensemble de la population. Il a également prouvé qu'il méritait la confiance qu'on lui témoignait.

À la fin des années quatre-vingt, il fut le premier à aborder le thème de la déjudiciarisation sur la place publique. Ce concept gagna la population et le gouvernement consacra de réels efforts à sa mise en oeuvre. Par exemple, afin d'aider à soulager l'appareil judiciaire et d'offrir à sa population un accès plus facile à la justice, le Législateur québécois a élargi, en 1998, les champs de compétence du notaire en matière non contentieuse. Il lui a en effet permis, en sa qualité d'officier public, de réaliser certaines procédures jusqu'alors réservées aux officiers de la Cour. Ainsi en est-il présentement dans les domaines de tutelle au mineur, d'ouverture de régime de protection au majeur, d'homologation de mandat donné en prévision de l'inaptitude ou de vérification de testament[15].

Peut-être parce qu'ils se percevaient menacés davantage que les autres par les nouvelles technologies de l'information, les notaires du Québec furent parmi les tout premiers juristes au Canada à s'y intéresser. En fait, apprivoisant les nouveaux paramètres, ils réalisèrent rapidement que loin de constituer un danger pour leur avenir en Amérique du Nord, la réalisation de transactions au moyen des technologies de pointe nécessiterait plus que jamais la présence des spécialistes de la sécurité juridique qu'ils étaient. D'ailleurs, ils reçurent bientôt l'invitation de l'*American Bar Association* pour joindre un comité chargé de promouvoir la création d'un nouveau professionnel du droit aux États-Unis : le *CyberNotary* . Les travaux de ce comité intéressent vivement plusieurs États américains[16]. « En effet, le Barreau américain mène des travaux visant à instaurer aux États-Unis la profession notariale afin qu'elle contribue à la mise en place d'un environnement propice au commerce électronique. Plusieurs des partenaires commerciaux des États-Unis sont des pays relevant de la tradition juridique romano-germanique qui est fondée sur la prééminence du droit écrit et de la preuve. Ils exigent, pour qu'il puisse prendre effet sur leur territoire, qu'un document juridique soit reconnu par un juriste indépendant comme conforme à la législation du lieu où il doit être applicable… Plusieurs transactions tardent sous prétexte que les documents soumis pour signature sont refusés par les partenaires commerciaux étrangers qui mettent en doute le caractère "indépendant" de l'avocat américain qui a rédigé la lettre d'opinion… Les juristes des États-Unis sont particulièrement séduits par l'idée d'être en mesure d'instaurer une catégorie de juristes capables de conférer l'authenticité aux actes qu'ils reçoivent afin d'éviter tout délai dans les transactions internationales auxquelles ils participent » [17].

Pour être en mesure de répondre en temps opportuns aux nouveaux besoins qui se manifesteraient bientôt, les notaires québécois créèrent, en juin 1996, une corporation sans but lucratif ayant pour mission de soutenir le développement technologique de la profession notariale : Notarius était née. Sa première tâche consista à relier l'ensemble de la profession par un intranet. Notarius mit ensuite en place une infrastructure à clés publiques destinée aux notaires. Ce service devint effectif et opérationnel le 4 mai 1999, faisant des notaires les premiers et encore les seuls professionnels détenteurs d'une

signature numérique. Ainsi, purent-ils se familiariser avec les fonctions de chiffrement et de signature numérique d'un document en devenant eux-mêmes utilisateurs de biclés pour la transmission, par voie électronique, de leurs rapports de testaments et de mandats au cas d'inaptitude à leur corporation professionnelle.

Les notaires utilisent également leur signature numérique pour leurs dossiers de financement hypothécaire avec certaines composantes du Mouvement Desjardins, dans le cadre d'un projet pilote en cours. Ce projet deviendra une entente permanente et s'étendra à l'ensemble du Québec avant la fin de l'année, une fois toutes les étapes du processus sous parfait contrôle. Depuis le début, c'est le secrétariat de la Chambre des notaires qui gère l'attribution des signatures numériques selon des conditions strictes et qui fait respecter les règles de leur utilisation.

Le notariat a également démontré son expertise par sa participation active à la réforme de la publicité foncière actuellement en voie de réalisation. Le ministère de la justice du Québec exécute ce projet en partenariat avec des firmes privées, dont Notarius. Ce partenariat « … a pour objet de définir la solution technologique et administrative nécessaire à la modernisation de la publicité foncière, d'élaborer l'architecture détaillée du système, de mettre au point la solution et de la mettre en place et d'exploiter le système informatique et de l'entretenir »[18]. « ce système permettra la consultation et l'inscription à distance, la gestion et la mise à jour du registre, la conservation des documents constituant le registre et la gestion de la version électronique de la documentation antérieure » [19]. « la sécurité des échanges électroniques sera assurée par une infrastructure à clé publique » [20]. Le concours de Notarius à cette réforme démontre bien ses compétences, mais lui procure aussi un bagage supplémentaire d'expériences qu'elle pourra faire profiter dans l'avenir.

Plus convaincante encore, parce que déjà éprouvée, est la collaboration du notariat au système de transmission électronique des réquisitions d'inscription au Registre des droits personnels et réels mobiliers (RDPRM). La direction de ce registre, contrairement à ses homologues des autres provinces, avait fait le pari d'offrir au public un mode de

transmission électronique qui soit pleinement sécuritaire. Pour le RDPRM, il importait d'assurer l'intégrité, l'intégralité et l'irréfutabilité des informations ainsi transmises[21]. L'identification certaine d'un requérant constituait donc l'une des premières pièces à intégrer au mécanisme de sécurité à mettre en place. Notarius démontra alors que les études notariales pourraient être ces comptoirs de vérification d'identité. Elle sut établir que les notaires possédaient les qualités d'impartialité, d'indépendance et de probité requises et que l'acte notarié en minute constituait l'instrument parfait pour assurer la véracité, la confidentialité et la pérennité de ces vérifications. C'est pourquoi le Gouvernement opta pour le notaire comme agent unique de la vérification d'identité et pour l'acte notarié en minute comme seule preuve acceptable de la constatation de cette vérification[22]. La disponibilité immédiate du service notarial sur tout le territoire québécois — plus de 1 500 points de services potentiels — et son expérience, récemment acquise, mais quasi exclusive, de la transmission électronique de documents chiffrés et signés furent assurément des arguments déterminants dans ce choix.

Après avoir reçu la formation obligatoire appropriée et l'accréditation nécessaire, plusieurs dizaines de notaires furent en mesure d'offrir ce service d'identification dès les premiers jours de l'introduction du nouveau mode de transmission. Aujourd'hui, c'est deux cent soixante-cinq notaires qui sont accrédités agents vérificateurs d'identités auprès du RDPRM et ce nombre ne cesse d'augmenter. Quoique la nouvelle procédure n'ait pas encore un an d'existence, on estime que les réquisitions acheminées par voie électronique représentent plus de quatre-vingt pour cent (80 %) du volume traité aujourd'hui[23].

Au Registre, on nous affirme que les plaintes de la clientèle à l'endroit des notaires se font rares et que les réticences, surtout manifestées au début du nouveau régime, s'estompent vite lorsque les usagers saisissent l'importance de la sécurité du processus. Par conséquent, on se dit très satisfait au RDPRM du service professionnel offert par les notaires et on est très fier, non sans raison, d'avoir obtenu le Prix Hommage 2000, Grandes organisations. Pour sa part, la Chambre des Notaires du

Québec est heureuse de participer à cette réussite qui suscite le plus grand intérêt ailleurs au Canada.

Le contexte international

En tant que pionnier dans l'application des technologies de pointe au monde juridique, le notariat québécois est lui aussi l'objet d'une attention particulière à l'extérieur de ses frontières. On a vu plus haut l'intérêt manifesté par l'*American Bar Association* . Soulignons de même l'attention portée par le notariat français[24]. et les autres membres qui composent L'Union Internationale du Notariat Latin. Cette organisation, qui regroupe les notaires de 67 pays, possède d'ailleurs sa commission sur l'informatique et la sécurité juridique. Le notariat d'ici entretient d'excellentes relations avec ces associations nationales et internationales — et avec bien d'autres — issues des deux principales traditions juridiques dans le monde. Combinées au leadership qu'il manifeste en matière technologique, ces relations constituent un atout de premier plan pour notre notariat dans la négociation et l'établissement de règles internationales de reconnaissance réciproque de services de certification et de répertoire. Nul doute qu'il s'agira là d'une particularité importante à considérer dans le choix de l'organisme chargé de la gestion de tels services.

Les nouvelles technologies de l'information ont contribué à faire éclater les frontières des échanges commerciaux. Les nations désirant légiférer dans ce secteur n'auront pas le choix de considérer cette conjoncture[25]. L'efficacité réelle d'une normalisation juridique d'un État se mesurera donc au taux de reconnaissance international des normes qu'il aura fixées. Tout en évitant de dénaturer ou de mettre en péril l'édifice législatif construit, elle s'appréciera aussi selon l'adaptation de ces dernières au contexte juridique et technologique mondial et à sa faculté d'accepter des équivalences. En ce sens, un organisme de certification et de répertoire présent, compétent et influent de la communauté juridique mondiale participera de façon plus efficace qu'un autre aux discussions et négociations internationales.

Conclusion

En définitive, nous pensons donc que le notariat québécois est pleinement en mesure, tant du point de vue technologique que du point de vue professionnel, d'assumer les services de certification et de répertoire traités à l'avant-projet de loi. Succinctement, la structure de ces services s'organiserait ainsi : les notaires seraient chargés de confirmer l'identité d'un requérant ou toute autre information pouvant faire l'objet d'un certificat[26]. Chaque confirmation serait réalisée d'après les critères de sécurité exigés selon les besoins en l'espèce. Ils constateraient cette vérification par acte authentique et transmettraient l'information à leur Ordre professionnel aux fins de la constitution du certificat. La Chambre des notaires du Québec serait responsable, quant à elle, en plus du contrôle traditionnel de la formation et du travail de ses membres, de la gestion complète des certificats. Cette gestion comprend la conservation et la délivrance des certificats, l'inscription de ceux-ci et des notaires vérificateurs dans un répertoire accessible au public et la confirmation de la validité des certificats répertoriés ainsi que leur association à une personne déterminée. Elle participerait également aux travaux visant l'harmonisation des systèmes et des normes, la certification entrecroisée et autres accords extra-territoriaux. Finalement, si tel est le vœu du Gouvernement, la Chambre des notaires pourrait également administrer le régime d'accréditation volontaire prévu à l'article 58 de l'avant-projet de loi.

Pour toutes les raisons indiquées ci-dessus, nous croyons sincèrement que ses caractères fondamentaux, son cadre, sa structure et son enracinement profond dans la société, alliés aux compétences particulières qu'elle a su développer par son dynamisme dans le domaine de la sécurité des échanges électroniques, illustrent avec éloquence l'aptitude de l'institution notariale québécoise à procurer les services de certification et de répertoire requis par l'avant-projet de loi.

---

1 Suzanne Thibodeau, Journal L'entracte, Vol. 5 n°13, p. 22.

2 Véronique Lépine, Les impacts juridiques liés à la dématérialisation des transactions commerciales, (2000) 6 R.E.J. 95, p. 110. Il est important de noter que l'auteure se questionne toutefois « …sur la pertinence d'une intervention relative à la mise sur pied d'une telle infrastructure de certification » (p. 112) jugeant que la

technologie de la cryptographie asymétrique serait suffisamment sécuritaire en elle-même. Voir aussi l'article 61 de l'avant-projet de loi.

3 En fait, la première manifestation législative de cette obligation apparaît à l'article 39 du Code du notariat (46 Vict., c. 32) sanctionné le 30 mars 1883. Voir à cet effet Julien S. Mackay, La Revue du notariat, Vol 91 no 9-10, p. 574.

4 Loi sur le notariat, article 41. Voir aussi Paul-Yvan Marquis, La responsabilité civile du notaire, Les Éditions Yvon Blais Inc., Cowansville, 1999, p. 310.

5 Règlement sur la tenue des dossiers et des études de notaires, article 21.3.

6 Loi sur le notariat, articles 2, 50 et 51.

7 Code de déontologie des notaires, articles 3.05.01 et 3.05.02.

8 Loi sur le notariat, article 15b).

9 Code des professions, article 23.

10 Règlement sur la souscription au Fonds d'assurance-responsabilité professionnelle de la Chambre des notaires du Québec, article 1.

11 Loi sur le notariat, article 2. Ces grands principes sont repris au projet de loi no 139 sur le notariat qui a été déposé récemment.

12 Suzanne Thibodeau, op. cit., note 1.

13 Pierre Ciotola, Journal L'Entracte, Vol. 4 no 1, p. 4.

14 Loi sur le notariat, article 2.

15 Code de procédure civile, articles 872, 874, 877.0.1, 878, 884.7 et 889

16 http://www.abanet.org/scitech/ec/cn/home.html et Benoît Longtin, Journal L'Entracte, Vol. 8 n° 9, p 3.

17 Benoit Longtin, op. cit., note 16. Comme partenaires commerciaux des États-Unis, citons par exemple, le Japon, l'Autriche, la Belgique, la France, l'Allemagne, la Grèce, l'Italie, le Luxembourg, les Pays-Bas, le Portugal, l'Espagne, la Hongrie, le Mexique, la Suisse, la Pologne et la Turquie, soit plus de 66% des pays faisant partie de l'Union Européenne et 58% des pays membres de l'Organisation de coopération et de développement économique (OCDE)

18 (18) Gilles Harvey, La réforme de la publicité foncière, (2000) 1 C.P. du N., p. 8

19 Gilles Harvey, op. cit., note 16, p. 11.

20 Gilles Harvey, op. cit., note 16, p. 12.

21 Martine Boivin, Les carrières du droit, Les éditions Ma Carrière, novembre 1999, p. 50.

22 Règlement sur le registre des droits personnels et réels mobiliers, article 15.1 et suiv.

23 D'après les chiffres disponibles au 30 juin 2000 et en tenant compte des réquisitions faites en vertu du droit transitoire, ce serait plus de 90 % des réquisitions qui seraient transmises par voie électronique au RDPRM.

24 « La capacité d'adaptation dont a fait preuve la profession outre-Atlantique (notariat québécois) n'est donc plus à démontrer : elle est à prendre en exemple. », Laurent Godemel, Le notaire, l'ordinateur et l'internet : vers la dématérialisation de l'acte authentique?, mémoire de fin de stage, diplôme supérieur du notariat, Faculté de droit, Université d'Auvergne, soutenance le 29 juin 1999, p. 41.

25 (25) À titre d'exemple, citons l'article 7 paragraphe 2 de la Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques (COM(98)0297 . C4-0376/98 . 98/0191 (COD)) : « Afin de promouvoir les services de certification transfrontaliers impliquant des pays tiers et la reconnaissance juridique des signatures électroniques émanant de pays tiers, la Commission peut, le cas échéant, présenter des propositions visant à l'instauration effective de normes et d'accords internationaux applicables aux services de certification. Elle peut notamment, si besoin est, soumettre au Parlement européen et au Conseil des propositions concernant des mandats de négociation d'accords bilatéraux et multilatéraux avec des pays tiers et des organisations internationales ».

26 Voir l'article 52 de l'avant-projet de loi.